Cyber-security incidents and audit quality

Pierangelo Rosati[1*] Fabian Gogolin[2] Theo Lynn[1]

[1] Irish Institute of Digital Business, DCU Business School, Dublin City University, Collins Avenue, Glasnevin, Dublin 9, Ireland.

[2] Leeds University Business School, University of Leeds, Woodhouse, Leeds, LS6 1AN, United Kingdom.

[*] Corresponding author: pierangelo.rosati@dcu.ie; phone: +353(1)7005253.

Forthcoming at European Accounting Review

Accepted by Chris Hogan
Date of first submission: 9 December 2018
Date of final acceptance: 17 November 2020

Acknowledgements
The research work described in this paper was supported by the Irish Centre for Cloud Computing and Commerce, an Irish national Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority, and by the Irish Institute of Digital Business. We thank Chris Hogan (Associate Editor), two anonymous reviewers, and the participants at the European Accounting Association Annual Meeting 2017 for their helpful comments and suggestions.

Abstract

As signals of internal control weaknesses, cyber security incidents can represent significant risk factors to the quality of financial reporting. We empirically assess the audit quality implications of data breaches for a large sample of US firms. Using a difference-in-difference approach based on a matched sample of breached and non-breached firms, we find no evidence that cyber-security incidents result in a decline in audit quality. Instead, we observe positive shifts in four widely-used proxies for audit quality. We document that breached firms (i) experience a decrease in abnormal accruals, (ii) are less likely to report small profits or small earnings increases, (iii) are more likely to be issued a going concern report, and (iv) are less likely to restate their financial statements in the two years following a breach. Our results indicate that auditors effectively offset increases in audit risk through additional substantive testing and audit effort. Our evidence supports the view that auditors have increased their audit risk awareness and put in place adequate procedures to deal with the consequences of cyber-security incidents.

Keywords: Cyber Security; External Audit; Audit Quality, SEC Comment Letter.

JEL Code: M41, M42, C30, K24.

1. Introduction

Accounting scandals at large publicly traded firms such as Enron and Worldcom, the demise of Arthur Andersen, and the passage of the Sarbanes-Oxley Act (SOX) of 2002 have increased the publics' and auditors' sensitivity to the risk of material errors and irregularities in financial statements. In this paper, we assess the implications of cyber-security incidents for audit quality. Existing research on how external auditors respond to cyber-security risks is limited and in particular questions concerning the impact on the quality of financial reporting remain unanswered. Cyber-security incidents are understood as signals for internal control weaknesses (Chernobai, Jorion, and Yu, 2011; Benaroch, Chernobai, and Goldstein, 2012; Benaroch and Chernobai, 2017) and, as such, can present significant risk factors to the quality of financial reporting (Hogan and Wilkins, 2008; Lawrence and Minutti-Meza and Vyas, 2018).

The number of cyber-security incidents is growing every year as a result of the increasing use of the Internet, mobile applications, and technologies such as cloud computing (Romanosky, Hoffman, and Acquisti, 2014; Abbasi, Sarker, and Chiang, 2016). Cyber-security incidents can result in significant damage to breached firms in terms of remediation costs, fines, and reputation (Cavusoglu, Mishra, and Raghunathan, 2004; Gordon, Loeb, and Zhou, 2011; Rosati, Deeney, Cummins, Van der Werff, and Lynn, 2019a). According to recent reports on cyber-security, more than 20 percent of firms that experience a security breach report a substantial loss of revenue, a reduction in their customer base, and lose out on business opportunities, with total costs amounting to approximately USD17 million per firm (CISCO 2017; Ponemon Institute 2016).

Firms establish internal control systems to provide reasonable assurance of reaching objectives in relation to operational effectiveness and efficiency, reliable financial reporting, and compliance with law and regulations (COSO, 2004). A cyber-security incident might directly affect and compromise the internal controls over financial reporting (ICFR) of the affected firm. In this case, firm's books and records may be altered, which could result in manipulations of the financial statements. This issue has recently been reiterated by regulators like the Public Company Accounting Oversight Board (PCAOB). The PCAOB specifically cautions external auditors to consider how cyber incidents may affect a firm's ICFR (PCAOB 2010, 2013).

However, given the integrated nature of firm's internal control systems, cyber-security incidents can also pose threats to audit quality through their effect on operational control risk, or in particular, information technology (IT) controls. Because operating and financial reporting activities rely on shared controls, a weakness in one area is likely to affect the other (Lawrence et al., 2018). Internal control weaknesses (Doyle, Ge, and McVay, 2007b; Ashbaugh-Skaife, Collins, Kinney, and LaFond, 2008), and IT control weaknesses in particular (Masli, Peters, Richardson, and Sanchez, 2010; Haislip, Masli, Richardson, and Sanchez, 2016; Messier, Eilifsen, and Austen, 2004; Klamm and Watson, 2009), can carry significant negative implications for financial reporting quality.

Recent research suggests that auditors respond to cyber-security incidents by increasing audit effort and charging higher audit fees to their clients (Li, No, and Boritz, 2016; Lawrence et al., 2018; Rosati, Gogolin, and Lynn, 2019b). There is also some evidence suggesting that cyber-security breaches can result in a higher likelihood of financial restatements in the year of the breach (Lawrence et al., 2018).

Our paper builds on this nascent stream of academic research and aims to provide additional insights in regard to the implications of cyber-security incidents for the quality of financial reporting. The aim of this paper is to provide a comprehensive empirical assessment of the change in audit quality around cyber-security events. We argue that, while internal control

weaknesses certainly increase audit risk, they may not necessarily result in a decrease in audit quality. For example, in the presence of internal control deficiencies, as inherent and control risks increase, auditors may increase their substantive testing to uphold the quality of the audit (Hogan and Wilkins, 2008). In line with this argument, previous research has identified an increase in audit fees as the result of cyber-security incidents (Li et al., 2016; Rosati et al., 2019b). To the extent, that audit fees serve as a proxy for audit effort (Whisenant, Sankaraguruswamy, and Raghunandan, 2003; Blankley, Hurtt, and MacGregor, 2012), the results imply that auditors, in the presence of cyber-security incidents, increase their audit effort to maintain an acceptable level of audit risk. The main argument of this paper is that if auditors increase their audit effort and substantive testing sufficiently, cyber-security incidents should not result in a reduction in audit quality.

We examine this assertion using a sample of 329 cyber-security incidents, affecting US listed companies, from 2005 to 2014, reported by Privacy Rights Clearinghouse (PRC). We limit our sample to firms audited by Big 4 auditors to ensure comparable levels of audit quality (Blankley et al., 2012; Rosati et al., 2019b), and match breached firms to non-breached firms operating within the same industry and with the nearest firm size (total assets). Throughout our analysis we adopt a difference-in-difference (DID) model design with year and industry fixed effects as per Rosati et al. (2019b), Khurana, Lundstrom, and Raman (2020), and Yu, Kwak, Park, and Zhang (2020), which allows us to assess the change in audit quality resulting from a cyber-security incident while also taking into account the staggered nature of these events. To assess the impact of cyber-security incidents on the quality of financial reporting, we examine a number of well-established proxies for audit quality, namely (i) the level of abnormal accruals, (ii) earnings benchmarks, (iii) the likelihood of issuing going-concern opinions, and (iv) the likelihood of financial restatements.

We find no evidence of a significant decrease in audit quality in the two years following a breach. This is an important finding because it supports the view that, despite being a significant risk factor, cyber-security breaches do not result in financial reporting deficiencies or audit failure. Instead, we document a significant and positive association between our measures of audit quality and cyber-security. We rationalise this result as a manifestation of the dynamic described by Li et al. (2016) and Rosati et al. (2019b). The authors observe an increase in audit fees as a function of increasing audit risk and audit effort. Following their rationale, we argue that the increased audit effort ultimately results in a positive post-incident effect (Li et al., 2016; Lawrence et al., 2018; Rosati et al., 2019b).

We also provide some analysis regarding one possible channel of transmission. Using SEC Comment Letters as proxies for regulator interest (Cassell, Dreher, and Myers, 2013), we show that breached firms are more likely to receive SEC Comment Letters and IT-related SEC Comment Letters following a cyber-security incident than non-breached firms. Indeed, regulatory scrutiny over clients can be a further incentive for auditors to increase their effort (Donohoe and Knechel, 2012; Bell, Causholli, and Knechel, 2015). As such, we argue that the increase in audit quality may be partially driven by pressures exerted from regulators, to which the auditor responds by increasing audit effort.

This study contributes to the growing literature on the impact and consequences of cyber-security incidents for external auditors and firms. First, this study specifically addresses the issue of audit quality, while previous related studies (Li et al., 2016; Lawrence et al., 2018; Rosati et al., 2019b) mostly focus on audit fees. Second, as opposed to previous studies that focus on a single audit quality indicator (Lawrence et al., 2018), we adopt a number of different proxies for audit quality to provide a more comprehensive assessment. Specifically, we examine the impact of cyber-security incidents on abnormal accruals, earnings benchmarks,

the likelihood of issuing going-concern opinions, and the likelihood of financial restatements. Third, our study also contributes to the literature on audit risk. Even though cyber-security incidents result in an increase in audit risk (Li et al., 2016; Rosati et al., 2019b), they do not prove to be detrimental to the quality of financial reporting. Our evidence provides support for the idea that auditors can decrease audit risk by increasing their audit effort. We also provide further evidence on the importance of SEC comment letters as an instrument of regulatory monitoring. Fourth, we provide further evidence on the importance of addressing sample bias and unobserved differences in treatment and control firms. Using a propensity score matched sample and a difference-in-difference approach to identify potential causal relationships, we are able to estimate on the relationship of cyber-security events and audit quality.

The remainder of the paper is organised as follows. In the next section, we discuss prior literature and present our hypothesis. This is followed by an outline of the research design and a description of the data used throughout this study. We then present the results, some robustness checks and a discussion of our empirical analysis. We conclude with some final remarks and avenues for future research.

2. Background and Hypothesis

2.1 Cyber-security incidents

The number of cyber-security incidents is growing every year particularly due to the increasing use of the Internet, cloud computing, and mobile devices (Romanosky et al., 2014; Abbasi et al., 2016). Cyber-security incidents can result in significant damage to breached firms in terms of remediation costs, fines, and reputation (Cavusoglu et al., 2004; Gordon et al., 2011; Rosati et al., 2019a). Cyber-security incidents are complex and multifaceted events and their full implications may not always materialise immediately. For example, Equifax, a credit-reporting agency, admitted on 7 September 2017, that hackers had compromised information of over 140 million individuals between May and July of the same year (Bernard, Hsu, Perlroth, and Lieber, 2017). Hackers were able to exploit a vulnerability of their website and gained access to social security numbers, dates of birth, driving licence numbers and credit card information. The consequences of the breach were considerable. The firm's stock price dropped approximately 18 percent upon first disclosure of the breach (Volz and Shepardson, 2017); court documents filed in the settlement of the case suggest that the minimum cost would be USD1.38 billion (Jaeger, 2020).

A number of empirical studies demonstrate that cyber-security incidents typically result in a loss in market value for the affected firms (Campbell, Gordon, Loeb, and Zhou, 2003; Cavusoglu et al., 2004; Gatzlaff and McCullough, 2010; Gordon et al., 2011; Kamiya, Kang, Kim, Milidonis, and Stulz, 2019; Rosati et al., 2019a). In extreme cases, the decline in a firm's market value can amount to 12 percent over a two-day period following the breach (Cavusoglu et al., 2004). In a recent study, Rosati et al. (2017) show that cyber incidents are also reflected in wider bid-ask spreads and abnormal trading volume. Overall, the evidence highlights the negative implications of cyber-security incidents (Campbell et al., 2003; Gatzlaff and McCullough, 2010; Gordon et al., 2011).

Extant research has identified a variety of contingency factors that can strengthen or weaken the observed market response to cyber-security incidents. Yayla and Hu (2011) and Das, Mukhopadhyay, and Anand (2012), for example, find that e-commerce firms are more severely affected by security breaches. Other factors that have been found to significantly affect the

market response to cyber-security breaches are firm size and type, industry, media coverage and disclosure texts (Acquisti, Friedman, and Telang, 2006; Yayla and Hu, 2011; Berezina, Cobanoglu, Miller, and Kwansa 2012; Das et al., 2012; Wang, Kannan, and Ulmer, 2013; Rosati et al., 2019a). Moreover, it is unclear whether and how the type of breach determines the strength of the market reaction as demonstrated by the inconclusive empirical evidence provided so far by academic researchers (Goldstein, Chernobai, and Benaroch, 2011; Gordon et al., 2011; Benaroch et al., 2012).

The implications of cyber-security incidents at firm- and market-level are well documented and articles about new breaches appear in the media on a regular basis. However, cyber-security incidents also affect a number of other stakeholders (Hovav and Gray, 2014). External auditors and regulators are particularly concerned about cyber-security incidents affecting firms under their supervision. Yet, this issue remains little explored in the literature.

2.2 Internal control weaknesses

Internal control is defined broadly as a process designed to provide reasonable assurance about the attainment of organisational objectives (COSO, 2013). An organisation establishes a system of internal control policies and procedures in response to the potential occurrence of events it has identified as posing a risk to its objectives (COSO, 2004). In this context, the occurrence of an adverse event would highlight a weakness in the internal control system, either because controls are missing or because they are deficient.

As a response to the large and high-profile accounting scandals that led to the implementation of SOX in 2002, the attention of regulators and the public on financial reporting risks has increased dramatically over the last decades. However, the breadth of internal controls spans beyond financial reporting as it also includes operations and regulatory compliance. As such, a firm's internal control system affects operational efficiency and effectiveness as well as financial reporting accuracy (Klamm and Watson, 2009). In this context, the impact of cyber-security incidents on the quality of financial reporting can be direct and indirect. Cyber-security risks can materialise in the form of so called "more-than-reporting" control weaknesses (Feng, McVay, and Skaife, 2014), such as IT control weaknesses or "financial reporting-only" weaknesses (Hogan and Wilkins, 2008).

The PCAOB suggests that external auditors are expected to consider how cyber-security events may affect a firm's internal control over financial reporting (ICFR). ICFR are designed "to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles" (PCAOB, 2014). It also considers procedures related to maintaining records, the documentation of transactions, authorisation of receipts and the safeguarding of assets (Hogan and Wilkins, 2008). Furthermore, Section 404 of SOX explicitly requires auditors to attest and report on the effectiveness of a client's ICFR. Prior research has linked cyber-security incidents to potential internal control weaknesses (Lawrence et al., 2018), and ICFR weaknesses to financial reporting deficiencies (e.g. Doyle, Ge, and McVay, 2007a; Ashbaugh-Skaife et al., 2008). It is thus clear, that in the event of a cyber-security incident that directly involves the firm's accounting systems, the auditor must carefully consider the risk of manipulation and the potential impact on financial statements (PCAOB, 2014).

However, cyber-security could also indirectly affect audit quality through their impact on a firm's operational controls. Control platforms such as system software, firm-level controls, and access controls, support entity-wide operating and control functions (IFAC, 2010). As such, it is not surprising that operational controls and financial reporting activities are heavily

integrated and rely on shared controls. This implies that weak operational controls likely pose a risk for financial reporting quality. In relation to cyber-security incidents, information technology (IT) controls are particularly relevant. Prior research shows that investments in IT can help automate processes and as a result reduce misstatements (Messier et al., 2004). However, different IT systems are now heavily integrated within the firm and through the Internet. As such, they also create additional risks if adequate IT controls are not in place which may ultimately result in material misstatements (Klamm and Watson, 2009).

Recent research finds that cyber-security incidents lead to a contemporaneous increase in audit fees (Li et al., 2016; Lawrence et al., 2018; Rosati et al., 2019b). Rosati et al. (2019b), for example, find that firms that experience a breach are charged 28 percent higher audit fees compared to non-breached firms in the year of a cyber-security incident. This increase is interpreted as a response to an increase in audit risk and audit effort. While the direction of the hypothesised impact of cyber-security events on audit risk is relatively clear (Li et al., 2016; Lawrence et al., 2018; Rosati et al., 2019b), the direction and effect on audit quality is not. The central argument of this paper is that, while cyber-security incidents may not necessarily be due to reporting deficiencies, they could be interpreted as a signals of potential control weaknesses (Benaroch and Chernobai, 2017), which would ultimately increase audit risk. When audit risk increases, auditors will increase their substantive testing to uphold the quality of the audit[1] (Hogan and Wilkins, 2008). As a result, if auditors perceive cyber-security incidents as signals of potential control weaknesses, they would increase their audit effort, and this would ultimately result in an increase in audit quality. Our research hypothesis is stated as follows:

Hypothesis: Breached firms experience an increase in audit quality following a cyber-security incident.

3. Research Methodology

3.1 Research Design

Cyber-security incidents may indicate potential internal control weaknesses (Chernobai et al., 2011; Benaroch et al., 2012). As such, they can trigger an increase in external monitoring, in particular from auditors (Doyle et al., 2007a; Hogan and Wilkins, 2008). In our analysis, we explore changes in audit quality in response to cyber-security incidents. Specifically, we consider four different measures for audit quality: (i) the level of abnormal accruals (Francis and Yu, 2009), (ii) earnings benchmarks (Francis and Yu, 2009), (iii) the likelihood of issuing going-concern opinions (Francis and Yu, 2009), and (iv) the likelihood of financial restatements (Blankley et al., 2012).

In order to test whether a significant difference between breached (treatment sample) and non-breached firms (control sample) exists before and/or after a cyber-security incident, we adopt a difference-in-difference (DID) approach in all our regression models (Lechner, 2011). The DID technique has been widely used in accounting studies (e.g. Cheng and Farber, 2008; Wang, 2010; Li et al., 2016; Zhang and Yu, 2016; Johnstone and Petacchi, 2017; Rosati et al., 2019b). DID is able to control for random causes of changes in the dependent variable over time while addressing heteroscedasticity and auto-correlation (Knechel and Sharma, 2012). As such, it is a powerful methodology to estimate causal relationships and to circumvent many endogeneity problems that can arise when comparing heterogeneous individuals or

[1] This point may be particularly relevant for Big4 auditors as they are assumed to possess a higher level of expertise (Haislip et al., 2016) and are associated with higher quality audits (DeAngelo, 1981).

organisations (Bertrand, Duflo, and Mullainathan, 2004; Johnston and Petacchi, 2017). We also included industry and year fixed-effects in all our models to take into account the staggered nature of cyber security incidents (Rosati et al., 2019b; Khurana et al., 2020; Yu et al., 2020).

The effect of a cyber-security incident may span over a number of years following an incident, we limit our analysis to a two years pre- and post-incident as per Rosati et al. (2019b). Because we are interested in the changes in financial reporting quality as a result of a cyber-security incident, we compare the value of our proxies for audit quality in the two years prior to the breach (-2; -1) and the two years following the breach (+1; +2). Rosati et al. (2019b) suggest that the year of a cyber-security incident is exceptional for the affected firm. In such events, the firm must deal with an immediate and critical situation with a potential increase in current and future costs. Similarly, the external auditor must increase the audit effort to ensure that the additional costs are properly recorded and that the reliability of the financial records are not impacted by the breach. In this context, the exclusion of the year of the breach (*t=0*) provides a cleaner empirical setting to examine changes in audit quality. Figure 1 provides a graphical representation of the timeline adopted in our analysis.

Insert Figure 1 here

3.2 Dependent Variables

3.2.1 Accruals Quality

Discretionary accruals are widely used to provide evidence of earnings management which is interpreted as a sign of lower audit quality (Francis and Yu, 2009). We used the following ordinary least-squares (OLS) regression model to estimate the discretionary component of accruals using the performance-adjusted Modified Jones model (Kothari, Leone, and Wasley, 2005). The model is estimated by fiscal year, two-digit industry (SIC code) while controlling for concurrent firm performance. The model takes the following form:

$$TA_{i,t} = \beta_0 + \beta_1 \Delta REV_{i,t} + \beta_2 PPE_{i,t} + \beta_3 NI_{i,t} + \varepsilon_{i,t} \quad (1)$$

The variables in the model are defined as follows: *TA* is total accruals; *ΔREV* is the change in revenues between year *t-1* and year *t*; *PPE* is gross property, plant, and equipment; and *NI* is operating income after depreciation. All variables are deflated by lagged total assets. The absolute value of the residuals (ε) from Equation (1) provides a measure of discretionary accruals following the rationale that individual firms may have incentives to engage in income-increasing or -decreasing earnings management (Warfield, Wild, and Wild, 1995)[2]. We use the absolute value of the residual as the dependent variable in the regression model presented in Equation (3).

As estimates, discretionary accruals are based on assumptions underlying the estimated model. In order to make sure that our results are not driven by the estimation bias of the selected model, we also estimate discretionary accruals using the Dechow and Dichev (2002) model. This model accounts for past (*t-1*), current (*t*) and future (*t+1*) cash flows. The model is specified as follows:

$$TA_{i,t} = \beta_0 + \beta_1 \Delta REV_{i,t} + \beta_2 PPE_{i,t} + \beta_3 CFO_{i,t-1} + \beta_4 CFO_{i,t} + \beta_5 CFO_{i,t+1} + \varepsilon_{i,t} \quad (2)$$

where *CFO* is the cash flow from operation while all other variables are as previously specified

[2] Becker, DeFond, Jiambalvo, and Subramanyam (1998) point out that auditors are more concerned about income-increasing rather than income-decreasing accruals since auditors are more likely to be sued for allegedly allowing overstated earnings. Therefore, we also considered "signed" accruals as an additional analysis and results are consistent.

in Equation (1). The absolute value of the residuals (ε) in Equation (2) provides the second measure of discretionary accruals and represents the dependent variable the regression model presented in Equation (3).

We combine the model proposed by Francis and Yu (2009)[3] with the staggered DID design adopted by Rosati et al. (2019b) to test whether accruals quality differs across breached and non-breached firms subsequent to a cyber-security incident:

$$\begin{aligned} ABS\_ACC_{i,t} = {} & \beta_0 + \beta_1 BREACHED_i + \beta_2 POST_{i,t} + \beta_3 BREACHED \times POST_{i,t} \\ & + \beta_4 BUS\_SEG_{i,t} + \beta_5 GEO\_SEG_{i,t} + \beta_6 LTA_{i,t} + \beta_7 SALESGROWTH_{i,t} \\ & + \beta_8 SALESGROWTH\_VOL_{i,t} + \beta_9 CFO_{i,t} + \beta_{10} CFO\_VOL_{i,t} \\ & + \beta_{11} MATWEAK_{i,t} + \beta_{12} LEV_{i,t} + \beta_{13} LOSS_{i,t} + \beta_{14} BANKRUPTCY_{i,t} \\ & + \beta_{15} MTB_{i,t} + \beta\ Industry\ Indicators + \beta\ Year\ Indicators + \varepsilon_{i,t} \end{aligned} \quad (3)$$

where:

ABS_ACC	=	the absolute value of the discretionary accruals estimated through the Modified Jones Model (*ABS_ACC_JM*) or through the Dechow-Dichev Model (*ABS_ACC_DD*)
BREACHED	=	indicator variable equal to 1 if a firm belongs to the treatment group (i.e. breached), 0 otherwise;
POST	=	indicator variable equal to 1 if the period is one or two years after a breach (*t+1* or *t+2*), 0 otherwise;
BREACHED x POST	=	interaction between *BREACHED* and *POST* (DID Estimator);
BUS_SEG	=	number of business segments;
GEO_SEG	=	number of geographic segments;
LTA	=	natural logarithm end of year total assets;
SALESGROWTH	=	one-year growth rate in sales;
SALESGROWTH_VOL	=	standard deviation of sales for the most recent three fiscal years;
CFO	=	operating cash flows;
CFO_VOL	=	standard deviation of cash flows for the most recent three fiscal years;
MATWEAK	=	indicator variable equal to 1 if a firm receives a material weakness opinion in the current or in the following year[4], 0 otherwise;
LEV	=	total debt divided by total assets;
LOSS	=	indicator variable equal to 1 if the income before extraordinary items is lower than zero, 0 otherwise;
BANKRUPTCY	=	Altman (2000) Z-Score;
MTB	=	Market to book ratio;
Industry Indicators	=	industry indicators based on two-digit SIC codes;
Year Indicators	=	year indicators;
ε	=	error term.

As outlined in Wooldridge (2010), the treatment dummy (i.e. *BREACHED*) captures possible differences in the level of accruals between the breached (treatment group) and non-breached

[3] The control variables related to auditor characteristics were excluded from the model as they were outside the scope of our study.

[4] This proxy for the effectiveness of internal control is consistent with the one used by Ettredge et al. (2006), Doyle et al. (2007a) and Blankley et al. (2012) which are also based on a two-year window. Blankley et al. (2012, p.84) point out that a two-year approach is necessary as "*there is a 'sticky' quality to internal controls so firms that received a material weakness in the future likely had weaker internal controls in the current year*". We also run all our regression models controlling for material weaknesses disclosed in the current year only to check the robustness of our results. Our conclusions were unaltered.

firms (control groups) before a breach occurs; the period dummy (i.e. *POST*) captures aggregate factors that may affect the level of accruals for both breached and non-breached firms; the DID estimator (*BREACHED x POST*) captures the difference between the change in the level of accruals pre- and post-breach for breached and non-breached firms. As an increase in audit quality is assumed to constrain the extent of earnings management, we expect the coefficient of our DID estimator (*BREACHED x POST*) to be negative.

We include control variables for many different firm characteristics as suggested by Francis and Yu (2009). Specifically, we control for: (i) the number of business (*BUS_SEG*) and geographical segments (*GEO_SEG*) firms operate in, since more diversified firms are more difficult to audit due to their complexity (Gul and Goodwin, 2010; Kim, Liu, and Zheng, 2012); (ii) firm size (*LTA*), since larger firms are subject to stricter monitoring and have stronger internal controls (Richardson, Tuna, and Wu, 2002; Balsam, Krishnan, and Yang, 2003; Gietzmann and Pettinicchio, 2014); (iii) sales growth (*SALESGROWTH*) and volatility of sales (*SALESGROWTH_VOL*) as they tend to be associated with lower earnings quality (Menon and Williams, 2004; Hribar and Nichols, 2007); (iv) operating cash flow and its volatility as larger (lower) cash flow (volatility) is usually associated with higher earnings quality (Dechow, Sloan, and Sweeney, 1995; Doyle et al., 2007b; Hribar and Nichols, 2007); (v) the level of internal controls (*MATWEAK*) since ineffective internal controls are associated with poor earnings quality (Doyle et al., 2007a); (vi) debt (*LEV*) and financial distress (*LOSS* and *BANKRUPTCY*) since debt covenants and poor financial conditions represent significant incentives to earnings manipulation (DeFond and Jiambalvo, 1994; Dichev and Skinner, 2002; Jaggi and Lee, 2002); and (vii) market-to-book ratio as firms with growth opportunities may have higher incentives to manage earnings in order to meet market expectations (Francis and Yu, 2009).

3.2.2 Earnings Benchmark

Previous studies suggest that meeting earnings expectations is one of the main incentives for earnings management (Healy and Wahlen, 1999) and that an abnormally high (low) proportion of firms report earnings just above or below the benchmarks (Burgstahler and Dichev, 1997; Degeorge, Patel, and Zeckhauser, 1999).

We combine the probit model proposed by Francis and Yu (2009) with the staggered DID design adopted by Rosati et al. (2019b) to test two common benchmarks: reporting small positive profits (avoiding losses), and reporting small positive earnings increases (avoiding earnings declines):

$$\begin{aligned} PROBIT[BENCHMARK = 1] = f(&\beta_0 + \beta_1 BREACHED_i + \beta_2 POST_{i,t} + \\ &+\beta_3 BREACHED \times POST_{i,t} + \beta_4 BUS\_SEG_{i,t} + \\ &+\beta_5 GEO\_SEG_{i,t} + \beta_6 LTA_{i,t} + \\ &+\beta_7 SALESGROWTH_{i,t} + \beta_8 SALESGROWTH\_VOL_{i,t} \\ &+\beta_9 CFO_{i,t} + \beta_{10} CFO\_VOL_{i,t} + \\ &+\beta_{11} MATWEAK_{i,t} + \beta_{12} LEV_{i,t} + \beta_{13} LOSS_{i,t} + \\ &+\beta_{14} BANKRUPTCY_{i,t} + \beta_{15} MTB_{i,t} + \\ &+\beta\ Industry\ Indicators + \\ &+\beta\ Year\ Indicators + \varepsilon_{i,t}) \end{aligned} \quad (4)$$

BENCHMARK is specified in two alternative ways: (i) an indicator variable equal to 1 if a firm reports a small profit (*SMALL_PROFIT*), and 0 otherwise; and (ii) an indicator variable equal to 1 if a firm reports a small earnings increase (*SMALL_INCREASE*), and 0 otherwise. We

adopt the definitions of small profit and earning increase proposed by Francis and Yu (2009). A firm is considered to report a small profit if its net income, deflated by lagged total assets, is between 0 and 5 percent, and to report a small earnings increase if the change in its net income, deflated by lagged total assets, is between 0 and 1.3 percent[5]. All other control variables are consistent with Francis and Yu (2009). The model is estimated using clustered robust standard errors to correct for heteroscedasticity and serial dependence (Rogers, 1993).

As per the model presented in Equation (3), *BREACHED*, *POST*, and *BREACHED x POST* are the variables of interest. Firms with higher audit quality are expected to be less likely to consistently meet earnings benchmarks. We expect the coefficient of *BREACHED x POST* to be negative if there is an increase in audit monitoring following a cyber-security incident.

3.2.3 Going Concern

Previous studies demonstrate that audit quality is associated with a higher probability of auditors issuing a going concern report (Francis, 2004; Knechel and Vanstraelen, 2007; Hardies, Breesch, and Branson, 2016).

In order to test whether the likelihood of issuing a going-concern audit report differs across breached and non-breached firms subsequent to a cyber-security incident, we adopt a combination of the probit model proposed by Francis and Yu (2009) and the staggered DID design adopted by Rosati et al. (2019b):

$$\begin{aligned} PROBIT[GCONCERN = 1] = f(&\beta_0 + \beta_1 BREACHED_i + \beta_2 POST_{i,t} + \\ &+\beta_3 BREACHED \times POST_{i,t} + \beta_4 BUS\_SEG_{i,t} + \\ &+\beta_5 GEO\_SEG_{i,t} + \beta_6 LTA_{i,t} + \\ &+\beta_7 CASH_{i,t} + \beta_8 PRIOR\_GCONCERN_{i,t} + \\ &+\beta_9 REPORT\_LAG_{i,t} + \beta_{10} LEV_{i,t} + \\ &+\beta_{11} LOSS_{i,t} + \beta_{12} LAG\_LOSS_{i,t} + \\ &+\beta_{13} BANKRUPTCY_{i,t} + \beta_{14} MTB_{i,t} + \\ &+\beta\ Industry\ Indicators \\ &+\beta\ Year\ Indicators + \varepsilon_{i,t}) \end{aligned} \quad (5)$$

GCONCERN is an indicator variable equal to 1 if a client receives a going-concern audit report, and 0 otherwise. *CASH* is a liquidity measure that is the sum of the firm's cash and investment securities, scaled by total assets. A firm with more liquid assets should be better able to deal with financial difficulties. Therefore *CASH* is expected to be negatively associated with the probability of a going-concern opinion (Francis and Yu, 2009). *PRIOR_GCONCERN* is an indicator variable equal to 1 if a firm received a going- concern opinion in the previous fiscal year as firms are more likely to receive a going-concern report if they received a prior-year going-concern qualification (Reynolds and Francis, 2000). *REPORT_LAG* measures the number of days between the fiscal year-end and the earnings announcement date as previous studies provide evidence of going-concern opinions being associated with longer reporting delays (Raghunandan and Rama, 1995; Carcello, Hermanson, and Huss, 1995; DeFond, Raghunandan, and Subramanyam, 2002). *LAG_LOSS* is an indicator variable equal to 1 if a firm reported a loss in the previous fiscal year, and 0 otherwise. All other control variables follow Francis and Yu (2009). As per the previous models, we estimate the regression coefficients using clustered robust standard errors to correct for heteroscedasticity and serial

[5] We also test our results using different thresholds i.e. 2 percent for small profit (Frankel, Johnson, and Nelson, 2002; Carey and Simnett, 2006), and between 1 and 2 percent for small earning increase (Frankel et al., 2002; Ashbaugh, LaFond, and Mayhew, 2003; Carey and Simnett, 2006). Our results are robust to these alternative specifications.

dependence (Rogers, 1993).

Given that firms with higher audit quality are expected to be more likely to receive a going concern report, we expect *BREACHED x POST* to have a positive coefficient.

3.2.4 Restatement

A restatement indicates low-quality financial reporting due to the incorrect application of accounting principles and is a strong indicator of low audit quality (Kinney, Palmrose, and Scholz, 2004; Francis, 2011; Eshleman and Guo, 2014).

We test whether the likelihood of disclosing a restatement differs across breached and non-breached firms following a cyber-security incident. We use the following probit model similar to the one adopted by Blankley et al. (2012) and combine it with the staggered DID design adopted by Rosati et al. (2019b):

$$\begin{aligned} PROBIT[RESTATE = 1] = f(&\beta_0 + \beta_1 BREACHED_i + \beta_2 POST_{i,t} + \\ &+\beta_3 BREACHED \times POST_{i,t} + \beta_4 LTA_{i,t} + \beta_5 LEV_{i,t} + \\ &+\beta_6 MTB_{i,t} + \beta_7 FIN_{i,t} + \beta_8 EPSGROW_{i,t} + \\ &+\beta_9 EPR_{i,t} + \beta_{10} CFO_{i,t} + \beta_{11} MATWEAK_{i,t} + \\ &+\beta_{12} ABAFEES_{i,t} + \beta\ Industry\ Indicators + \\ &+\beta\ Year\ Indicators + \varepsilon_{i,t}) \end{aligned} \quad (6)$$

RESTATE is an indicator variable equal to 1 if a firm restates its financial statements within a two-year period (*t+1* or *t+2*) and 0 otherwise as per Blankely et al. (2012)[6]. Capital markets can generate incentives for aggressive accounting practices (Healy and Wahlen, 1999), hence we control for two market-related factors that are associated with restatements, namely growth expectations, measured as earnings-to-price ratio (*EPR*) and market-to-book ratio (*MTB*), and demand for external financing, measured as the sum of additional cash raised from issuance of long-term debt, common stock and preferred stock scaled by total assets (*FIN*) and cash-flow from operations (*CFO*) (Richardson et al., 2002). We also include a control variable (*EPSGROW*) for the pressure of maintaining a positive earnings trend since such a pressure might represent an incentive to earnings manipulation (Myers, Myers, and Skinner, 2007). Finally, we include control variables for the level of internal controls (*MATWEAK*) and audit effort, measured as abnormal audit fees (*ABAFEES*)[7]. Both variables are included because previous research has linked ineffective internal control (Feldmann, Read, and Abdolmohammadi, 2009) and low audit effort to the likelihood of a firm to restate (Blankley et al., 2012). All other control variables are as per Blankley et al. (2012). We adopt clustered robust standard errors to correct for heteroscedasticity and serial dependence (Rogers, 1993).

Stricter audit monitoring typically leads to higher audit quality, which should ultimately result in a lower probability of restatement (Blankley et al., 2012). Hence, we expect the coefficient of *BREACHED x POST* to have a negative coefficient if breached firms experience an increase

[6] A restatement is the alteration of previously audited financial statements due to errors, frauds or other causes (Stanley and DeZoort, 2007). As such, it represents a late manifestation of poor audit quality as errors or misreporting in the financial statement were not detected during the initial audit.

[7] We use the model suggested by Blankley et al. (2012) to estimate abnormal audit fees. In the model, the dependent variable is the natural logarithm of audit fees and the results suggest that larger (LTA), riskier (CR, CA_TA, LOSS, LEV, INTANG MATWEAK), and more complex (FOREIGN, SEG, MERGER) firms pay higher audit fees, while more profitable firms (ROA), and firms whose fiscal year end on December 31st pay lower audit fees. These results are consistent with Blankley et al. (2012) and with prior literature on audit fees which suggests that audit fees depend on auditee's size, complexity, risk, financial condition and internal controls (Simunic, 1980; Craswell, Francis, and Taylor, 1995; Gul and Goodwin, 2010; Gietzmann and Pettinicchio, 2014; Han, Rezaee, Xue, and Zhang, 2016; Rosati et al. 2019b). The regression results are reported in Appendix B.

in audit quality following a cyber-security incident.

3.3 Sample Selection

Our sample is based on all cyber-security incidents reported by Privacy Rights Clearinghouse (PRC) from 2005 to 2014. PRC is a California based non-profit corporation that aims to identify trends in privacy protection and communicate its findings to advocates, policymakers, industry, media and consumers. PRC also maintains detailed information about cyber security incidents in the US. Information about the incidents is collected through either government agencies or verifiable media sources. Even though the list cannot be considered exhaustive because "many organisations are not aware they have been breached or are not required to report it based on reporting laws" (PRC, 2017), previous studies have demonstrated its value for academic research (Garrison and Ncube, 2011; Higgs, Pinsker, Smith, and Young, 2016; Li et al., 2016; Rosati et al., 2017, 2019a, 2019b). Furthermore, the widespread adoption of Security Breach Notification Laws (SNBLs)[8] across different states, their increasing disclosure requirements, and the fact that PRC gathers information from multiple information sources, mitigates the potential sampling bias.

This dataset contains 4,041 cyber-security incidents disclosed by firms, non-profit organisations, healthcare organisations and government agencies in the US from April 2005 to December 2014. We restrict our sample to incidents that affect publicly traded firms. Further, we excluded financial firms (SIC Codes 6000-6999) due the different nature of their financial statements[9], and firms audited by auditors other than the Big4 in order to ensure relative homogeneity in audit quality (Blankley et al., 2012). Finally, in order to avoid the influence of previous incidents, we include only the first cyber-security breach for each firm in our sample. The final sample (hereafter also referred to as 'treatment' sample) consists of 329 breached firms.

In order to minimise potential changes in external monitoring due to firm's characteristics other than cyber-security incidents, we employ propensity score matching (PSM) in all our analyses as implemented by Lawrence et al. (2018). First, we estimate the probability of a firm becoming a breach target (Equation 7). We then match each breached firm (treatment) with a non-breached firm (control sample) within the same industry and with closest probability of being breached in the fiscal year of a cyber-security incident (with no replacement)[10]. Our probability model follows the model outlined in Lawrence et al. (2018):

[8] SBNLs require "notification (1) in a timely manner (2) if personally identifiable information has either been lost, or is likely to be acquired, by an unauthorised person, (3) and is reasonably considered to com- promise an individual's personal information" (Romanosky, Telang, and Acquisti, 2011, p. 257). Since 2002, when the first SBNL was enacted California, 47 states Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted their own SNBLs (NCSL, 2017).

[9] This is a standard practice in quantitative accounting studies as financial companies have different reporting requirements and the structure of their financial statement is difficult to compare with the one of non-financial firms (Fama and French, 1992; Dechow, Hutton, Kim and Sloan, 2012). The reported financial statements for banks, for example, are somewhat different from most companies as there are no accounts receivables or inventory to gauge whether sales are rising or falling (Francis and Wang, 2008). Also, as Gore, Pope, and Singh (2001, p. 15) pointed out, "the accrual generating process in financial firms is fundamentally different from that in industrial and commercial firms".

[10] Rosati et al. (2019b) adopts a more restrictive matching condition i.e. a maximum distance of three percent in the estimated score between breached and the corresponding matched firm. Even though such restrictive condition ensures more similarity between matched firms, it also causes a significant reduction in sample size. In order to preserve the size of our sample we opt for a Nearest-Neighbour approach. We also repeated our analyses using the more restrictive matching condition implemented in Rosati et al. (2019b) which reduced our breached sample to 248. Our main conclusions were unaltered.

$$PROBIT[BREACH = 1] = f(\beta_0 + \beta_1 MATWEAK_{i,t} + \beta_2 SIZE_{i,t} + \beta_3 AGE_{i,t} + \beta_4 ROA_{i,t} + \beta_5 LOSS_{i,t} + \beta_6 LEV_{i,t} + \beta_7 SEGMENTS_{i,t} + \beta_8 ACQUISITIONS_{i,t} + \beta_9 SALESGROWTH_{i,t} + \beta_{10} SPECIALIST_{i,t} + \beta\ Industry\ Indicators + \beta\ Year\ Indicators + \varepsilon_{i,t}) \quad (7)$$

BREACH is an indicator variable equal to 1 if a firm experiences a cyber-security incident in year *t*, and 0 otherwise. *SIZE* is the natural logarithm of the firm's market capitalisation at the fiscal-year end. *AGE* is the natural logarithm of 1 plus the number of years the firm is listed on Compustat. *ROA* is the return on assets, calculated as net income in the fiscal year scaled by total assets. *SEGMENTS* is the natural logarithm of 1 plus the number of operating and geographic segments at the fiscal year-end. *ACQUISITIONS* is the aggregate dollar value of acquisitions in the previous fiscal year (*t-1*) scaled by market capitalisation at the end of the current fiscal year (*t*). *SPECIALIST* is an indicator variable equal to 1 if the firm's auditor has the highest market share in the client's industry, measured using audit fees in fiscal year t, and 0 otherwise. We retrieve accounting information from the Compustat Fundamentals Annual file, and audit and restatement data from Audit Analytics. Following Blankley et al. (2012), we eliminate from these original files (i.e. pre-matching) (i) firms that failed to issue an internal control opinion, (ii) foreign filers since they were not required to issue an internal control opinion prior to July 2007, and (iii) restatements caused by clerical errors.

Table 1 provides a summary of the sample construction (Panel A) and the frequency of cyber-security incidents by year (Panel B).

Insert Table 1 here

4. Results and Discussion

4.1 Descriptive Statistics

Table 2 provides the descriptive statistics for the variables used in our analysis and the t-tests on differences between breached and non-breached firms. The results show some interesting insights in relation to the dependent variables of our regression models. Breached firms in our sample are more likely to receive SEC Comment Letters than non-breached firms. This may suggest that breached firms are subject to stricter regulator monitoring than non-breached firms. However, this relationship is not confirmed by other variables as no significant difference between breached and non-breached firms emerges in relation to abnormal accruals, the likelihood of reporting small profits or small income increases, the likelihood of receiving a going concern report, or to issue a restatement.

Our results further suggest that breached firms tend to have higher risk of default (*HIGHBANKRUPTCY*), to be more diversified (*BUS_SEG*), to rely more on external financing (*FIN*) and to have higher earnings to price ratios (*EPR*), to take shorter time to report financial results (*REPORT_LAG*), and finally to have more liquid assets (*CASH*) than non-breached firms. Further, breached firms tend to pay higher abnormal audit fees (*ABAFEES*), which also suggests they may be subject to stricter auditor monitoring (Blankley et al., 2012). We observe no significant difference in the size and other important firm-level controls, suggesting that our matching procedure effectively addressed the heterogeneity between breached and non-breached firms. We also performed a correlation analysis in order to verify whether there was a risk of multicollinearity between the control variables included in our regression models. The correlation coefficients are reported in Appendix C. These are consistent with previous studies

and do not show presence of any strong correlation[11] which might lead to multicollinearity.

Insert Table 2 here

4.2 Accruals quality

Table 3 presents the results of the regression model presented in Equation (3). The dependent variable in Panel A (*ABS_ACC_JM*) is the absolute value of abnormal accruals estimated using the Modified Jones Model (Dechow et al., 1995). The dependent variable in Panel B (*ABS_ACC_DD*) is the absolute value of abnormal accruals estimated using the Dichow-Dichev Model (Dichow and Dichev, 2002). An increase in abnormal accruals is typically associated with lower audit monitoring and therefore lower audit quality. The main variables of interest for our analysis are *BREACHED*, *POST* and the DID estimator *BREACHED x POST*. The coefficient of *BREACHED* is positive but not significant suggesting that there is no significant difference between breached and non-breached firms in terms of abnormal accruals before the breach. Similar conclusions can be drawn for *POST* which suggest that no difference emerges in the full sample between pre- and post-incident periods. The coefficient of the DID estimator *BREACHED x POST* is negative and significant suggesting that, *ceteris paribus,* breached firms experience a decrease in abnormal accruals following a cyber-security incident compared to non-breached firms. These results are consistent with our hypothesis that breached firms are subject to stricter auditor monitoring following a cyber-security incident. The results are consistent across different accruals models (Panel A and B).

Other results suggest that firms with higher sales growth rate (*SALESGROWTH*) and financial leverage (*LEV*) tend to report larger abnormal accruals, while firms with larger assets (*LTA*), and firms with larger cash flows (*CFO*) or reporting losses (*LOSS*) tend to report lower abnormal accruals. These results are largely consistent with previous studies (e.g. Francis and Yu, 2009).

The DID design relies on the assumption that the trend in the outcome variables for both the treatment and control groups in the pre-event period should be similar; this is also called parallel trend assumption. Following Tang, Mo, and Chan (2017), we tested the parallel trend assumption in two ways. First, we plot the distributions of abnormal accruals for treatment and control firms between the two periods using Kernel density. The plots show that the distributions are similar pre-incident. Second, we performed a Kolmogorov-Smirnov test, a non-parametric test for the equality of distributions. The test suggests that there is no significant difference in the distributions of the abnormal accruals pre-incident (p-value=0.526 for Panel A and p-value=0.911 for Panel B), and hence the parallel trend assumption is not violated .

Insert Table 3 here

4.3 Earnings benchmark

Table 4 reports the results of the regression model presented in Equation (4). The dependent variable in Panel A (*SMALL_PROFIT*) is an indicator variable equal to 1 if a firm reported a net income deflated by lagged total assets between 0 and 5 percent; the dependent variable in Panel B (*SMALL_INCREASE*) is an indicator variable equal to 1 if a firm reported a change in net income deflated by lagged total assets is between 0 and 1.3 percent (Francis and Yu, 2009). A lower probability of reporting small profits or small earnings increases is typically associated

[11] A Pearson correlation coefficient higher than 0.6 denotes a strong correlation which might bias the estimation of the regression coefficients (see Gujarati 2003, Ch. 10 for further discussion).

with higher earnings quality and therefore with higher audit quality and stricter audit monitoring. In line with the results discussed in Section 4.2, the coefficients of *BREACHED* and *POST* are not statistically significant. This suggests that no significant difference exists between breached and non-breached firms during the full sample period, or between pre- and post-incident periods for the full sample. The coefficient *BREACHED x POST* is negative and significant in both panels suggesting that breached firms have a lower probability of reporting small profits or small earnings increases after a cyber-security incident compared to non-breached firms. On the basis of the marginal effects associated with the regression coefficients, breached firms have a 2.70 percent lower probability of reporting small profits and a 2.90 percent lower probability of reporting small earnings increases than non-breached firms after an incident. These results are consistent with our hypothesis that breached firms are subject to stricter auditor monitoring following a cyber-security incident and are robust to a range of different proxies for earnings benchmarks. Also, the Kolmogorov-Smirnov test suggests that the parallel trend assumption is valid (p-value=0.899 for Panel A and p-value=0.992 for Panel B in Table 4).

Other results presented in Table 4 suggest that larger firms, firms with higher cash flow volatility (*CFO_VOL*) and with lower probability of default (*BANKRUPTCY*), or firms reporting losses (*LOSS*) are, *ceteris paribus*, less likely to constantly meet their earnings benchmarks. On the contrary, firms with internal control weaknesses (*MATWEAK*) are more likely to constantly meet those benchmarks.

Insert Table 4 here

4.4 Going concern opinion

Table 5 reports the results of the regression model presented in Equation (5). In this model, the dependent variable (*GCONCERN*) is an indicator variable equal to 1 if a firm received a going-concern audit report, and 0 otherwise. The coefficients of *BREACHED* and *POST* are once again not statistically significant suggesting that breached and non-breached firms have a similar probability of receiving a going-concern report over the sample period and that such probability does not change significantly for the full sample in the post-incident period. However, the coefficient of *BREACHED x POST* is positive and statistically significant suggesting that breached firms have a 2.66[12] percent higher probability of receiving a going-concern opinion following a cyber-security incident compared to non-breached firms. As higher audit quality is assumed to be positively correlated with the probability of a client receiving a going-concern report, this result is consistent with our hypothesis that breached firms are subject to stricter auditor monitoring following a cyber-security incident. The Kolmogorov-Smirnov test suggests that the parallel trend assumption is valid (p-value=0.999).

Other results suggest that, *ceteris paribus*, more diversified (*GEO_SEG* and *BUS_SEG*) and larger firms (*LTA*), and firms with more liquid assets (*CASH*) are less likely to receive a going-concern report, while firms that have received a going-concern report in the past (*PRIOR_GCONCERN*), are also more likely to receive another report.

Insert Table 5 here

4.4 Restatements

Table 6 reports the results of the regression model presented in Equation (6). The dependent

[12] This is based on the marginal effect associated with the regression coefficient.

variable (*RESTATE*) is an indicator variable equal to 1 if a firm discloses a restatement within the following two years and 0 otherwise. The coefficients of *BREACHED* and *POST* are both positive but non-significant, while the coefficient of the DID estimator (*BREACHED x POST*) is negative and significant. These results suggest that a negative and significant difference emerges between breached and non-breached firms following a cyber-security incident. Based on the corresponding marginal effects, *ceteris paribus*, breached firms have a 8.44 percent lower probability of a restatement than non-breached firms following an incident. The differences to the results reported in Lawrence et al. (2018) may be due to a number of reasons. Firstly, Lawrence et al. (2018) include the year of the breach in their analysis. As discussed in Section 3.1, the breach year represents an exceptional year both for the client and the auditor and may affect the results of the regression analysis. Secondly, their modelling approach differs from ours as they use a panel model with year and industry fixed-effects. As such, their empirical setup does not account for differences in breached or non-breached firms. Thirdly, systematic differences in the size of breached and non-breached firms are not well captured in the panel model presented by Lawrence et al. (2018); recent evidence suggests that firm size indicators are significantly related to a firm's probability of being breached (Kamiya et al., 2020).

As higher audit quality is associated with a lower probability of restatement (Blankley et al., 2012), our results provide further evidence that breached firms are subject to stricter auditor monitoring following a cyber-security incident. The Kolmogorov-Smirnov test suggests that the parallel trend assumption is valid (p-value=0.983) for our research design.

Other coefficients suggest that the probability of future restatements is higher for firms with ineffective internal controls (*MATWEAK*), while it is lower for larger firms (*LTA*) and firms with larger earnings-to-price ratio (*EPR*). These results are consistent with Blankley et al. (2012) and provide further evidence of the negative impact of poor internal controls on financial reporting quality (Klamm and Watson, 2009; Blankley et al., 2012; Klamm, Kobelsky, and Watson, 2012).

Insert Table 6 here

4.5 Additional analysis: SEC comment letters

Our results provide evidence that breached firms experience an increase in audit quality in the two years after a cyber-security incident. An increase in audit quality is typically associated with an increase in audit effort, ultimately resulting in lower audit risk (Caramanis and Lennox, 2007). However, given the special attention regulators attribute to cyber-security, breached firms are likely to be closely monitored. Increased regulatory scrutiny likely extends to the activities of the external auditors as they are responsible for testing the internal controls of their clients. Previous studies suggest that auditors are likely to increase their effort when their clients are subject to higher regulatory scrutiny (e.g. Donohe and Knechel, 2012; Bell et al., 2015). We hypothesise a similar dynamic in the context of cyber-security incidents. Therefore, we extend our analysis and examine whether breached firms are subject to higher regulatory scrutiny, measured as the probability of receiving an SEC Comment Letter (Cassell et al., 2013).

Following the Sarbanes-Oxley Act (SOX) of 2002, the Division of Corporation Finance at the SEC must review all issuers at least once every three years. Comment Letters represent the primary regulatory instrument for the SEC to request additional information about items in the financial statements, disclosure practices and internal controls (Gietzmann and Pettinicchio,

2014; Johnstone and Petacchi, 2017). While SEC Comment Letters predominantly relate to annual and quarterly financial reports, material news disclosures, proxy statements, and registration and prospectus filings (Dechow, Lawrence, and Ryans, 2015), they can also cover topics like risk factor disclosure and information security (Rosati et al., 2019b).

We retrieve SEC Comment Letters from Audit Analytics and consider both: (i) the probability of receiving a general SEC comment letter (i.e. regardless the topic of the enquiry), and (ii) the probability of receiving an SEC Comment Letter specifically focused on IT-related issues[13]. The assumption here is that if breached firms attract higher regulatory scrutiny, they should have a higher probability of receiving a Comment Letter. Following Cassell et al. (2013)[14] and the staggered DID approach adopted for the other models (Rosati et al., 2019b), we test this assumption using a probit model with clustered robust standard errors to correct for heteroscedasticity and serial dependence (Rogers 1993):

$$\begin{aligned} PROBIT[CL = 1] = f(&\beta_0 + \beta_1 BREACHED_i + \beta_2 POST_{i,t} + \\ &+\beta_3 BREACHED \times POST_{i,t} + \beta_4 MATWEAK_{i,t} \\ &+\beta_5 LTA_{i,t} + \beta_6 LOSS_{i,t} + \beta_7 HIGHBANKRUPTCY_{i,t} + \\ &+\beta_8 SALEGROWTH_{i,t} + \beta_9 BUS\_SEG_{i,t} + \\ &+\beta\ Industry\ Indicators + \beta\ Year\ Indicators + \varepsilon_{i,t} \end{aligned} \quad (8)$$

CL is an indicator variable equal to 1 if a firm receives an SEC Comment Letter within the following two years and 0 otherwise[15]. Similar to our main regression models, *BREACHED*, *POST*, and *BREACHED x POST* are the variables of interest. The model includes a number of control variables: (i) material weaknesses (*MATWEAK*) since firms disclosing material weaknesses are subject to higher monitoring than firms with effective internal controls (Doyle et al., 2007a; Johnston and Petacchi, 2017); (ii) firm size (*LTA*) since larger firms receive more attention from auditors and regulators than smaller firms and therefore are more likely to receive a comment letter (Fernando, Abdel-Meguid, and Elder, 2010; Cassell et al., 2013); (iii) firm's profitability (*LOSS*) since previous studies suggest that less profitable firms have lower financial reporting quality and therefore might be subject to higher scrutiny from regulators (Walker and Casterella, 2000; Cassell et al., 2013); (iv) financial distress (*HIGHBANKRUPTCY*) since distressed firms are more likely to be subject to additional monitoring than non-distressed firms (Cassell et al., 2013); and (v) firm's complexity (*SALEGROWTH* and *BUS_SEG*) since more complex firms are more difficult to audit (Cassell et al., 2013).

The results are reported in Table 7. The probability of receiving an SEC Comment Letter (*CL*) is the dependent variable in Panel A, while the probability of receiving an IT-related SEC Comment Letter (*CL_IT*) is the dependent variable in Panel B.

In Panel A, the coefficient of *BREACHED* and *POST* are non-significant while the coefficient

[13] The topics in the Comment Letters were identified on the basis of a proprietary taxonomy implemented in Audit Analytics. We define IT-related Comment Letters as those letters covering the topic 'Data Protection and Security Breach' as classified by Audit Analytics (Rosati et al., 2019b).

[14] Cassell et al. (2013) adopt a logistic regression to test their hypothesis. As an additional test, we performed the same analysis using a logistic regression and results are consistent.

[15] Our approach is similar to the one adopted by Cassell et al. (2013) who measure the variables that represent specific events or changes over a three-year window. This is justified by the fact that the SEC is required to review the 10-K filing of each registrant at least once every three years (see Section 408 paragraph (c) of the Sarbanes-Oxley Act). The SEC then issues a Comment Letter when a filing is found to be materially deficient or when further clarifications are needed. While Cassell et al. (2013) focus on the extent of the comments received and the cost associated with Comment Letters, and therefore consider the events occurred in the previous three years which may have put the firm under the SEC spotlight, we consider a cyber-security incident as one of those events because it may signal potential internal control weaknesses and therefore attract higher regulatory scrutiny. In other words a cyber-security incident in year *t* may trigger a Comment Letter in year *t+1* or *t+2*.

BREACHED x POST is positive and significant. This suggests that breached firms have a 10 percent higher probability of receiving an SEC Comment Letter than non-breached firms after experiencing a cyber-security incident. The results in Panel B are mostly consistent as the coefficients of *BREACHED* and *POST* are negative and non-significant while the coefficient of *BREACHED x POST* is positive and significant. Our results suggest that breached firms are more likely to receive this type of Comment Letters following a cyber-security incident. Specifically, the probability is 9.2 percent higher for breached firms when compared to non-breached firms. The results of this additional analysis provide evidence supporting a general increase in regulatory scrutiny following cyber-security incidents. Interestingly, the results are stronger (although marginally) for general Comment Letters than for IT-related Comment Letters. This indicates that the SEC tends to question auditors and managers about their financial reporting rather than their IT-related practices. Overall, the results of our analyses suggest that the increase in audit quality in breached firms may partly derive from an increase in audit risk and regulatory scrutiny.

Insert Table 7 here

5. Robustness Tests

Although we adopt a variety of audit quality proxies throughout our analysis, we perform a number of additional robustness tests. First, we introduce IT-related control weaknesses as an additional control in all our models. IT-related control weaknesses have been found to be positively related to misstatements (Klamm and Watson, 2009) and, as such, may increase cyber-security risk (Klamm and Watson, 2009; Cereola and Cereola, 2011). We also re-run our analysis and exclude our proxy for internal control weakness to avoid potential multicollinearity. In both cases the results are consistent with those presented in previous sections. Second, we test our models using a different specification of *RESTATE* and *CL*. Specifically, we test restatements and Comment Letters announced within one year instead of within two years as suggested by Lawrence et al. (2018). Our conclusions remain unchanged. Thirdly, we run our analysis on the subsample of events that occurred after the release of the first SEC disclosure guidance on cyber-security in 2011 (SEC, 2011). While the long time period allows us to work with a larger sample, more recent events may generate different outcomes than events that lie further in the past (Gordon et al., 2011). The results and conclusions based on a subsample of breaches since 2011 are consistent with those discussed in the main analysis. Fourthly, we also test whether the results of our analyses depend on the length of the time period considered. To address these concerns, we run the same analyses considering three and four years[16] before and after an incident and the results are consistent. Finally, in order to further validate our results, we also carried out personal interviews with five senior IT auditors from the Big 4 audit firms[17] who confirmed that they revise their audit plan following a cyber-security incident, and that they pay extra attention to breached clients in the years following a cyber-security incident. Finally, the interviewees also clarified that the revision of the audit plan tends to be incremental rather than radical. Additional testing, indeed, is mainly focused on the weaknesses highlighted by incidents; this usually allows auditors to collect additional valuable audit evidence leading to higher audit quality.

6. Summary and Conclusion

[16] We limit the number of years pre- and post-incident as the longer the time period the higher the likelihood of a firm experiencing another breach.
[17] One from Ernst&Young, KPMG and PricewaterhouseCoopers, and two from Deloitte.

Based on a sample of publicly listed US firms, this study demonstrates that cyber-security incidents do not result in an observable deterioration in audit quality. We document consistent positive shifts in four commonly used audit quality proxies. This is an important finding which supports the view that, despite being a significant risk factor, cyber-security breaches do not result in financial reporting deficiencies. We understand our findings as the result of the documented increase in audit effort in Li et al. (2016) and Rosati et al. (2019b). In respect to a possible channel of transmission, we show that breached firms are subject to higher regulatory scrutiny than non-breached firms. Therefore, regulatory scrutiny, as a side effect of cyber-security incident, may partially explain the observed increase in audit quality.

The documented results may be of relevance and interest for managers, auditors and policy makers. Managers may benefit from a better understanding of the potential consequences of cyber-security incidents beyond mere direct and tangible costs like fines, loss in revenues etc. Auditors may be interested in the results of this study as an external assessment of the effectiveness of their practices in response to cyber-security incidents. Finally, our study also has policy implications. It shows that auditors are able to sufficiently address and respond to cyber-security risks even in the absence of specific disclosure requirements[18] from regulators.

Our study is also subject to a number of limitations which may represent avenues for future research. First, our sample of data breaches is not exhaustive. It covers only a sample of publicly listed US firms. The fact that cyber-security incidents at large US firms do not lead to an observable deterioration in audit quality cannot easily be generalised. While large US firms may have a higher likelihood of becoming a breach target in the first place, they also have readily available resources to deal with the consequences of a breach. Similarly, we only focus on Big 4 auditors. The Big 4 may have more expertise in dealing with cyber-risk than non-Big 4 auditors (DeAngelo, 1981, Haislip et al., 2016). An analysis of non-Big 4 auditors and their ability to address cyber-security incidents may lead to substantially different results and conclusions. Second, we do not address whether the type and the extent of a cyber-security incident influences the auditor and regulator's response. Previous studies in the information management literature find that incident characteristics, such as breach type or the type of data stolen, result in different market reactions and costs (Campbell et al., 2003; Cavusoglu et al., 2004; Gatzlaff and McCullough, 2010; Gordon, Loeb, and Sohail, 2010; Rosati et al., 2019a). Auditors may also perceive some incidents as less severe than others and therefore adjust their audit effort accordingly. An in-depth analysis of the characteristics of a breach may help address this point. Third, due to technological innovation, outsourcing information systems and the adoption of cloud computing has increased over the last decade (Han and Mithas, 2013; Rosati and Lynn, 2016). Both outsourcing and cloud computing represent a significant challenge for auditors, particularly because of an increase in potential material weaknesses (Klamm et al., 2012) or the risk of failure in financial reporting due to the provider's errors (Anderson, Christ, Dekker, and Sedatole, 2014). Qualitative and quantitative research may provide useful insights in respect to auditors' perception of these recent trends. Given that the literature on the relationship between cyber-security and audit risk is at an early stage, this paper provides the foundation for future research in this field. Finally, aggregated data from Audit Analytics does not allow us to disentangle the effect of audit risk and regulatory monitoring as potential triggers of increased audit effort. Future studies leveraging more in-depth information about auditors' activities may shed light on this matter and provide further insights concerning auditors' proactiveness or reactiveness to cyber-security incidents.

[18] The Securities and Exchange Commission (SEC) issued guidelines on the disclosure of cyber-risk in 2011 (SEC 2011). However, specific regulatory requirements for cyber-security risk disclosure were only enacted on 26 February 2018 (SEC 2018).

References

Abbasi, A., Sarker, S. and Chiang, R. H. (2016). Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *Journal of the Association for Information Systems,* 17 (2), 1-22.

Acquisti, A., Friedman, A. and Telang, R., (2006). *Is there a cost to privacy breaches? An event study*. Proceedings of the International Conference on Information Systems (ICIS) 2006.

Anderson, S. W., Christ, M. H., Dekker, H. C., and Sedatole, K. (2014). The use of management controls to mitigate risk in strategic alliances: Field and survey evidence. *Journal of Management Accounting Research*, 26(1), 1-32.

Ashbaugh, H., LaFond, R., and Mayhew, B. W. (2003). Do nonaudit services compromise auditor independence? Further evidence. *The Accounting Review*, 78(3), 611-639.

Ashbaugh-Skaife, H., Collins, D. W., Kinney Jr, W. R., and LaFond, R. (2008). The effect of SOX internal control deficiencies and their remediation on accrual quality. *The Accounting Review*, 83(1), 217-250.

Balsam, S., Krishnan, J. and Yang, J. S. (2003). Auditor industry specialization and earnings quality. *Auditing: A Journal of Practice and Theory*, 22(2), 71-97.

Becker, C., DeFond, M., Jiambalvo, J., and Subramanyam, K. R. (1998). The effect of audit quality on earnings management. *Contemporary Accounting Research*, 15(1), 1–24.

Bell, T. B., Causholli, M., and Knechel, W. R. (2015). Audit firm tenure, non-audit services, and internal assessments of audit quality. *Journal of Accounting Research*, 53(3), 461-509.

Benaroch, M., and Chernobai, A. (2017). Operational IT failures, IT value-destruction, and board-level IT governance changes. Available at SSRN: https://ssrn.com/abstract=2887773.

Benaroch, M., Chernobai, A. and Goldstein, J., (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting Information Systems*, 13(4), 357-381.

Berezina, K., Cobanoglu, C., Miller, B.L. and Kwansa, F.A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, 24(7), 991-1010.

Bernard, T. S., Hsu, T, Perlroth, N., and Lieber, R. (2017). Equifax Says Cyberattack May Have Affected 143 Million in the U.S.. New York Times (September 7, 2018). Available at: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html (last accessed December 8, 2018).

Bertrand, M., Duflo, E., and Mullainathan, S. (2004). How much should we trust differences-in-differences estimates?. *The Quarterly Journal of Economics*, 119(1), 249-275.

Blankley, A. I., Hurtt, D. N. and MacGregor, J. E. (2012). Abnormal audit fees and restatements. *Auditing: A Journal of Practice & Theory,* 31(1), 79-96.

Burgstahler, D., and Dichev, I. (1997). Earnings management to avoid earnings decreases and losses. *Journal of Accounting and Economics*, 24(1), 99–126.

Campbell K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431-448.

Caramanis, C., and Lennox, C. (2008). Audit effort and earnings management. *Journal of Accounting and Economics*, 45(1), 116-138.

Carey, P., and Simnett, R. (2006). Audit partner tenure and audit quality. *The Accounting Review*, 81(3), 653-676.

Carcello, J. V., Hermanson, D. R., and Huss, H. F. (1995). Temporal changes in bankruptcy-related reporting. *Auditing*, 14(2), 133.

Cassell, C. A., Dreher, L. M., and Myers, L. A. (2013). Reviewing the SEC's review process: 10-K comment letters and the cost of remediation. *The Accounting Review*, 88(6), 1875-1908.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 70-104.

Cereola, S. J., and Cereola, R. J. (2011). Breach of data at TJX: An instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation. *Issues in Accounting Education*, 26(3), 521-545.

Cheng, Q., and Farber, D. B. (2008). Earnings restatements, changes in CEO compensation, and firm performance. *The Accounting Review*, 83(5), 1217-1250.

Chernobai, A., Jorion, P., and Yu, F. (2011). The determinants of operational risk in US financial institutions. *Journal of Financial and Quantitative Analysis*, 46(6), 1683-1725.

Cisco (2017). Cisco 2017 Annual Cyber security Report. Available at: https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html (last accessed December 8, 2018).

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004). *Enterprise Risk Management —Integrated Framework*. Durham, NC: AICPA.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2013). *Internal Control—Integrated Framework*. Durham, NC: AICPA.

Das, S., Mukhopadhyay, A. and Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, 8(4), 27-55.

DeAngelo, L. E. (1981). Auditor size and audit quality. *Journal of Accounting and Economics*, 3(3), 183-199.

Dechow, P. M., and Dichev, I. D. (2002). The quality of accruals and earnings: The role of accrual estimation errors. *The Accounting Review*, 77(1), 35-59.

Dechow, P. M., Hutton, A. P., Kim, J. H., and Sloan, R. G. (2012). Detecting earnings management: A new approach. *Journal of Accounting Research*, 50(2), 275-334.

Dechow, P. M., Lawrence, A., and Ryans, J. P. (2015). SEC comment letters and insider sales. *The Accounting Review*, 91(2), 401-439.

Dechow, P. M., Sloan, R. G., and Sweeney, A. P. (1995). Detecting earnings management. *The Accounting Review*, 70(2), 193-225.

DeFond, M. L., Raghunandan, K., and Subramanyam, K. R. (2002). Do non–audit service fees impair auditor independence? Evidence from going concern audit opinions. Journal of Accounting Research, 40(4), 1247-1274.

Degeorge, F., Patel, J., and Zeckhauser, R. (1999). Earnings management to exceed thresholds. *The Journal of Business*, 72(1), 1-33.

Dichev, I. D., and Skinner, D. J. (2002). Large–sample evidence on the debt covenant hypothesis. *Journal of Accounting Research*, 40(4), 1091-1123.

Donohoe, M. P., and Knechel, R. W. (2014). Does corporate tax aggressiveness influence audit pricing?. *Contemporary Accounting Research*, 31(1), 284-308.

Doyle, J. T., Ge, W., and McVay, S. (2007a). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44(1), 193-223.

Doyle, J. T., Ge, W., and McVay, S. (2007b). Accruals quality and internal control over financial reporting. *The Accounting Review*, 82(5), 1141-1170.

Eshleman, J. D., and Guo, P. (2014). Do Big 4 auditors provide higher audit quality after controlling for the endogenous choice of auditor?. *Auditing: A Journal of Practice & Theory*, 33(4), 197-219.

Ettredge, M. L., Li, C., and Sun, L. (2006). The impact of SOX Section 404 internal control quality assessment on audit delay in the SOX era. *Auditing: A Journal of Practice & Theory*, 25(2), 1-23.

Fama, E. F., and French, K. R. (1992). The cross-section of expected stock returns. *The Journal of Finance*, 47(2), 427-465.

Feldmann, D. A., Read, W. J., and Abdolmohammadi, M. J. (2009). Financial restatements, audit fees, and the moderating effect of CFO turnover. *Auditing: A Journal of Practice & Theory*, 28(1), 205-223.

Feng, M., Li, C., McVay, S. E., and Skaife, H. (2014). Does ineffective internal control over financial reporting affect a firm's operations? Evidence from firms' inventory management. *The Accounting Review*, 90(2), 529-557.

Fernando, G. D., Abdel-Meguid, A. M., and Elder, R. J. (2010). Audit quality attributes, client size and cost of equity capital. *Review of Accounting and Finance*, 9(4), 363-381.

Francis, J. R. (2004). What do we know about audit quality?. *The British Accounting Review*, 36(4), 345-368.

Francis, J. R. (2011). A framework for understanding and researching audit quality. *Auditing: A Journal of Practice & Theory*, 30(2), 125-152.

Francis, J. R., and Yu, M. D. (2009). Big 4 office size and audit quality. *The Accounting Review*, 84(5), 1521-1552.

Francis, J. R., and Wang, D. (2008). The joint effect of investor protection and Big 4 audits on earnings quality around the world. *Contemporary Accounting Research*, 25(1), 157-191.

Frankel, R. M., Johnson, M. F., and Nelson, K. K. (2002). The relation between auditors' fees for nonaudit services and earnings management. *The Accounting Review*, 77(s-1), 71-105.

Garrison, C. P., and Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230.

Gatzlaff, K. M., and McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, 13(1), 61-83.

Gietzmann, M. B., and Pettinicchio, A. K. (2014). External auditor reassessment of client business risk following the issuance of a comment letter by the SEC. *European Accounting Review*, 23(1), 57-85.

Goldstein, J., Chernobai, A. and Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems,* 12(9): 606-631.

Gordon, L. A., Loeb, M. P., and Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 567-594.

Gordon, L. A., Loeb, M. P., and Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33-56.

Gore, J. P. O., Pope, P. F., and Singh, A. (2001). *Non-audit services, auditor independence and earnings management*. Lancaster University Management School Working Paper 2001/014.

Gujarati, D. N. (2003). *Basic Econometrics*. New York: McGraw-Hill.

Gul, F. A., and Goodwin, J. (2010). Short-term debt maturity structures, credit ratings, and the pricing of audit services. *The Accounting Review*, 85(3), 877-909.

Haislip, J. Z., Masli, A., Richardson, V. J., and Sanchez, J. M. (2016). Repairing Organisational Legitimacy Following Information Technology (IT) Material Weaknesses: Executive Turnover, IT Expertise, and IT System Upgrades. *Journal of Information Systems*, 30(1), 41-70.

Han, K., and Mithas, S. (2013). Information Technology Outsourcing and Non-IT Operating Costs: An Empirical Investigation. *MIS Quarterly*, 37(1), 315-331.

Han, S., Rezaee, Z., Xue, L., and Zhang, J. H. (2016). The association between information technology investments and audit risk. *Journal of Information Systems,* 30(1), 93-116.

Hardies, K., Breesch, D., and Branson, J. (2016). Do (fe)male auditors impair audit quality? Evidence from going-concern opinions. *European Accounting Review*, 25(1), 7-34.

Healy, P. M., and Wahlen, J. M. (1999). A review of the earnings management literature and its implications for standard setting. *Accounting Horizons,* 13(4), 365-383.

Higgs, J.L., Pinsker, R.E., Smith, T.J., and Young, G.R. (2016). The Relationship between Board-Level Technology Committees and Reported Security Breaches. *Journal of Information Systems,* 30(3), 79-98.

Hogan, C. E., and Wilkins, M. S. (2008). Evidence on the audit risk model: Do auditors increase audit fees in the presence of internal control deficiencies? *Contemporary Accounting Research*, 25(1), 219-242.

Hovav, A., and Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the Association for Information Systems*, 34, pp. 894-913.

Hribar, P., and Nichols, G. D. (2007). The use of unsigned earnings quality measures in tests of earnings management. *Journal of Accounting Research*, 45(5), 1017-1053.

International Federation of Accountants (IFAC) (2010). Guide to Using International Standards on Auditing in the Audits of Small- and Medium-Sized Entities. Available at: https://www.ifac.org/system/files/publications/files/guide-to-using-internationa-1.pdf (last accessed December 8, 2018).

Jaggi, B., and Lee, P. (2002). Earnings management response to debt covenant violations and debt restructuring. *Journal of Accounting, Auditing and Finance*, 17(4), 295-324.

Johnston, R., and Petacchi, R. (2017). Regulatory oversight of financial reporting: Securities and Exchange Commission comment letters. *Contemporary Accounting Research*, 34(2), 1128-1155.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M., 2020. What is the impact of successful cyberattacks on target firms?. *Journal of Financial Economics*, Forthcoming.

Khurana, I. K., Lundstrom, N., and Raman, K. K. (2020). PCAOB Inspections and the Differential Audit Quality Effect for Big 4 and Non-Big 4 US Auditors. *Contemporary Accounting Research* (forthcoming).

Kim, J. B., Liu, X., and Zheng, L. (2012). The impact of mandatory IFRS adoption on audit fees: Theory and evidence. *The Accounting Review*, 87(6), 2061-2094.

Kinney, W. R., Palmrose, Z. V., and Scholz, S. (2004). Auditor Independence, Non-Audit Services, and Restatements: Was the US Government Right?. *Journal of Accounting Research*, 42(3), 561-588.

Klamm, B. K., and Watson, M. W. (2009). SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems*, 23(2), 1-23.

Klamm, B. K., Kobelsky, K. W., and Watson, M. W. (2012). Determinants of the persistence of internal control weaknesses. *Accounting Horizons*, 26(2), 307-333.

Knechel, W. R., and Sharma, D. S. (2012). Auditor-provided nonaudit services and audit effectiveness and efficiency: Evidence from pre-and post-SOX audit report lags. *Auditing: A Journal of Practice & Theory*, 31(4), 85-114.

Knechel, W. R., and Vanstraelen, A. (2007). The relationship between auditor tenure and audit quality implied by going concern opinions. *Auditing: A Journal of Practice & Theory*, 26(1), 113-131.

Kothari, S. P., Leone, A. J., and Wasley, C. E. (2005). Performance matched discretionary accrual measures. *Journal of Accounting and Economics*, 39(1), 163-197.

Lawrence, A., Minutti-Meza, M., and Vyas, D. (2018). Is Operational Control Risk Informative of Financial Reporting Deficiencies?. *Auditing: A Journal of Practice & Theory*, 37(1), 139-165.

Lechner, M. (2011). The estimation of causal effects by difference-in-difference methods. *Foundations and Trends® in Econometrics*, 4(3), 165-224.

Li, H., No, W. G., and Boritz, J. E. (2016). Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. Working Paper. SSRN: 2880928.

Masli, A., Peters, G. F., Richardson, V. J., and Sanchez, J. M. (2010). Examining the potential benefits of internal control monitoring technology. *The Accounting Review*, 85(3), 1001-1034.

Jaeger, J. (2020). Equifax must spend 'a minimum of $1B' for data security. . Reuters (January 21, 2020). Available at: https://www.complianceweek.com/cyber-security/equifax-must-spend-a-minimum-of-1b-for-data-security/28329.article (last accessed September 20, 2020).

Menon, K., and Williams, D. D. (2004). Former audit partners and abnormal accruals. *The Accounting Review*, 79(4), 1095-1118.

Messier, W. F., Eilifsen, A., and Austen, L. A. (2004). Auditor detected misstatements and the effect of information technology. *International Journal of Auditing*, 8(3), 223-235.

Myers, J. N., Myers, L. A., and Skinner, D. J. (2007). Earnings momentum and earnings management. *Journal of Accounting, Auditing and Finance*, 22(2), 249-284.

National Conference of State Legislature (NCSL) (2017). *Security Breach Notification Laws*. Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last accessed July 26, 2017).

Ponemon Institute (2016). *Cost of Data Breach Study: Global Analysis*. Available at: https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-1995&S_PKG=ov49542 (last accessed December 8, 2018).

Privacy Rights Clearinghouse (PRC) (2017). *Chronology of Data Breaches: FAQ*. Available at: https://www.privacyrights.org/chronology-data-breaches-faq (last accessed July 29, 2017).

Public Company Accounting Oversight Board (2OB) (2010). *Identifying and Assessing Risks of Material Misstatement*. AS No. 12: Public Company Accounting Oversight Board (PCAOB).

Public Company Accounting Oversight Board (PCAOB) (2013). *Considerations for Audits of Internal Control over Financial Reporting*: Public Company Accounting Oversight Board (PCAOB).

Public Company Accounting Oversight Board (PCAOB) (2014). *Auditing Standard No. 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements*: Public Company Accounting Oversight Board (PCAOB)

Raghunandan, K., and D. Rama. 1995. Audit opinions for companies in financial distress: Before and after SAS No. 59. Auditing: *A Journal of Practice & Theory*, 14, 50–63.

Reynolds, J. K., and Francis, J. R. (2000). Does size matter? The influence of large clients on office-level auditor reporting decisions. *Journal of Accounting and Economics*, 30(3), 375-400.

Richardson, S., Tuna, I., and Wu, W. (2002). *Predicting Earnings Management: The Case of Earnings Restatements*. Working paper, University of Pennsylvania.

Rogers, W. (1993). Regression standard errors in clustered samples. *Stata technical bulletin*, 13, 19-23.

Romanosky, S., Hoffman, D., and Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1): 74-104.

Romanosky, S., Telang, R., and Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, 30(2), 256-286.

Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., and Lynn, T. (2019a). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, *47*, 458-469.

Rosati, P., Deeney, P., Gogolin, F., Cummins, M., van der Werff, L., and Lynn, T. (2017). The Effect of Data Breach Announcements Beyond The Stock Price: Empirical Evidence on Market Activity. *International Review of Financial Analysis*, 49, 146-154.

Rosati, P., Gogolin, F., and Lynn, T. (2019b). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. *The International Journal of Accounting*, *54*(03), 1950013.

Rosati, P., and Lynn, T. (2016). AIS: Challenges to Technology Implementation. In: *AIS Companion*, edited by: M. Quinn, and E. Strauss, Routledge.

Securities and Exchange Commission (SEC) (2011). CF Disclosure Guidance: Topic No. 2 – Cybersecurity. Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (last accessed December 8, 2018).

Securities and Exchange Commission (SEC) (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf (last accessed December 8, 2018).

Simunic, D. A. (1980). The pricing of audit services: Theory and evidence. *Journal of Accounting Research*, 18(1), 161-190.

Stanley, J. D., and DeZoort, F. T. (2007). Audit firm tenure and financial restatements: An analysis of industry specialization and fee effects. *Journal of Accounting and Public Policy*, 26(2), 131-159.

Tang, T., Mo, P. L. L., and Chan, K. H. (2017). Tax collector or tax avoider? An investigation of intergovernmental agency conflicts. *The Accounting Review*, 92(2), 247-270.

Volz, D., and Shepardson, D. (2017). Criticism of Equifax data breach response mounts, shares tumble. Reuters (September 8, 2017). Available at: https://www.reuters.com/article/us-equifax-cyber/equifax-shares-slump-after-massive-data-breach-idUSKCN1BJ1NF (last accessed December 8, 2018).

Walker, P. L., and Casterella, J. R. (2000). The role of auditee profitability in pricing new audit engagements. *Auditing: A Journal of Practice and Theory*, 19(1), 157-167.

Wang, X. (2010). Increased disclosure requirements and corporate governance decisions: Evidence from chief financial officers in the pre-and post–Sarbanes-Oxley periods. *Journal of Accounting Research*, 48(4), 885-920.

Warfield, T., Wild, J., and Wild, K. (1995). Managerial ownership, accounting choices, and informativeness of earnings. *Journal of Accounting and Economics*, 20(1), 61–91.

Whisenant, S., Sankaraguruswamy, S., and Raghunandan, K. (2003). Evidence on the joint determination of audit and non-audit fees. *Journal of Accounting Research*, 41(4), 721-744.

Wooldridge, J. M. (2010). Econometric analysis of cross section and panel data. MIT Press.

Yayla, A.A. and Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, 26(1): 60-77.

Yu, J., Kwak, B., Park, M. S., and Zang, Y. (2020). The Impact of CEO/CFO Outside Directorships on Auditor Selection and Audit Quality. *European Accounting Review* (forthcoming).

Zhang, J. Z., and Yu, Y. (2016). Does board independence affect audit fees? Evidence from recent regulatory reforms. *European Accounting Review*, 25(4), 793-814.

FIGURE 1

Timeline of the DID analysis

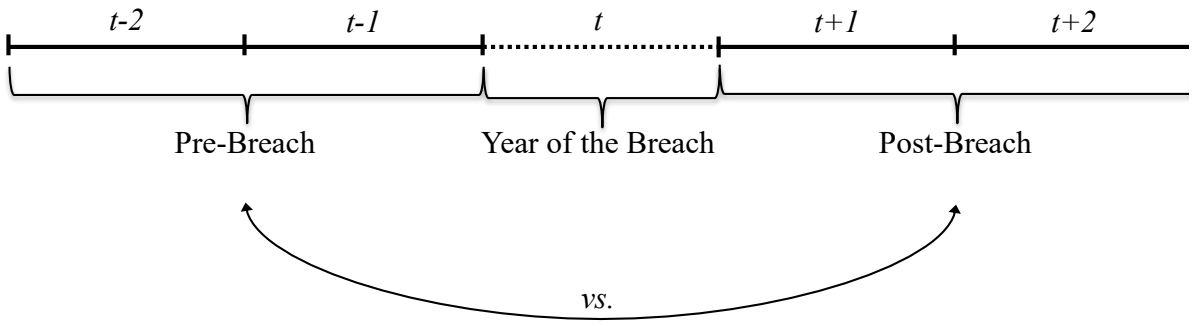

TABLE 1

Sample Composition

Panel A: Sampling process

Cyber Security Incidents	**Firms**
Events reported by Privacy Rights Clearinghouse (2005–2014)	4,041
Non-publicly traded firms	(3,619)
Financial Companies	(83)
Non-Big 4	(10)
Final sample (Treatment)	329
Financial and Audit Information	
Compustat Fundamental Annual	13,455
Financial Companies	(1,998)
Audit Analytics Restatement File	5,833
Missing Data	(1,069)
Remaining	4,764
Final Sample (Control)	329

Panel B: Cyber-security incidents by year

Year	**No. of breaches**	**Percentage**
2005	18	5.47
2006	47	14.29
2007	34	10.33
2008	23	6.99
2009	23	6.99
2010	36	10.94
2011	42	12.77
2012	39	11.85
2013	42	12.77
2014	25	7.60
Total	329	100.00

This table summarises the sampling process (Panel A) and reports the number of cyber-security incidents per year (Panel B).

TABLE 2
Descriptive Statistics and Tests of Differences

Variable	Overall	Breached	Non-Breached	Diff.	t-statistic	p-value	
CL	0.506	0.539	0.480	0.059	2.78	0.005	***
CL_IT	0.012	0.014	0.011	0.002	0.57	0.570	
ABS_ACC_JM	0.774	0.786	0.762	0.024	0.11	0.913	
ABS_ACC_DD	0.868	0.831	0.903	-0.072	-0.41	0.684	
SMALL_PROFIT	0.279	0.265	0.291	-0.026	-1.34	0.179	
SMALL_INCREASE	0.244	0.241	0.246	-0.005	-0.29	0.767	
GCONCERN	0.004	0.005	0.004	0.001	0.33	0.735	
PRIOR_GCONCERN	0.005	0.004	0.005	-0.001	-0.42	0.676	
RESTATE	0.103	0.104	0.102	-0.002	-0.18	0.858	
LAF	15.849	15.869	15.833	0.037	0.66	0.506	
ABAFEES	0.200	0.279	0.127	0.153	4.77	0.000	***
LTA	16.468	16.452	16.482	-0.030	-0.69	0.509	
LEV	0.206	0.214	0.200	0.014	1.28	0.199	
LOSS	0.153	0.159	0.147	0.009	0.62	0.532	
LAG_LOSS	0.139	0.146	0.132	0.014	0.85	0.396	
BANKRUPTCY	2.893	2.899	2.887	0.012	0.04	0.965	
HIGHBANKRUPTCY	0.028	0.039	0.020	0.019	2.65	0.008	***
SALESGROWTH	1.095	1.086	1.101	-0.015	-0.94	0.344	
SALESGROWTH_VOL	0.568	0.615	0.520	0.095	1.39	0.165	
BUS_SEG	0.648	0.686	0.617	0.068	2.14	0.032	**
GEO_SEG	1.568	1.560	1.575	-0.015	-0.71	0.475	
MTB	3.300	4.267	2.289	1.979	1.64	0.101	
FIN	0.115	0.126	0.107	0.019	1.79	0.073	*
EPSGROW	0.518	0.530	0.508	0.021	1.03	0.302	
EPR	0.000	0.000	0.000	0.000	3.28	0.001	***
CFO	0.056	0.058	0.054	0.003	1.03	0.302	
CFO_VOL	0.037	0.036	0.038	0.002	-0.99	0.921	
MATWEAK	0.034	0.034	0.035	-0.001	-0.09	0.921	
REPORT_LAG	102.512	96.259	107.568	-11.308	-3.95	0.000	***
CASH	0.162	0.179	0.150	0.029	2.95	0.003	***

This table reports the descriptive statistics of the variables adopted in the empirical analysis and t-test on the differences between breached and non-breached firms. All the variables are defined in Appendix A. P-values denote the level of significance of t-Tests under the null hypothesis of equal means in the subsamples of breached and non-breached firms. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

TABLE 3
Regression Results: Audit Quality – Earnings Management

	Panel A: Modified Jones Model				Panel B: Dechow-Dichev Model			
Variable	**Coeff.**	**t-statistic**	**p-value**		**Coeff.**	**t-statistic**	**p-value**	
INTERCEPT	3.191	1.65	0.098	*	5.840	3.91	0.000	***
BREACHED	0.145	0.82	0.415		0.046	0.16	0.873	
POST	0.028	0.64	0.520		0.132	0.95	0.343	
BREACHED x POST	-0.168	-3.54	0.000	***	-0.124	-4.28	0.000	***
BUS_SEG	0.018	0.09	0.928		0.018	0.12	0.906	
GEO_SEG	0.003	0.70	0.453		0.007	0.12	0.907	
LTA	-0.002	-1.96	0.050	**	-0.003	-4.23	0.000	***
SALESGROWTH	0.043	2.68	0.008	***	0.030	2.62	0.009	***
SALESGROWTH_VOL	0.000	0.50	0.617		0.000	2.16	0.031	**
CFO	-0.102	-1.80	0.072	*	-0.237	-0.25	0.800	
CFO_VOL	0.013	0.29	0.773		0.027	0.84	0.404	
MATWEAK	0.196	2.32	0.021	**	0.157	1.20	0.230	
LEV	0.048	1.66	0.097	*	0.015	2.94	0.003	***
LOSS	-0.037	-2.02	0.045	**	-0.067	-1.91	0.057	*
BANKRUPTCY	0.018	0.53	0.599		0.014	0.17	0.867	
MTB	0.000	0.06	0.951		0.003	0.81	0.421	
Industry fixed-effect		Yes				Yes		
Year fixed-effect		Yes				Yes		
F-Stat		6.07				6.67		
p-value		0.000				0.000		
Adjusted R-squared		0.23				0.25		
N		2,632				2,632		

This table reports the results of the OLS regression analysis for the model presented in Equation (3). Regression coefficients are estimated using Newey-West robust standard errors to correct for heteroscedasticity and first-order autocorrelation. The dependent variable in Panel A (Panel B) is the absolute value of abnormal accruals estimated using the Modified Jones Model (Dehow-Dichev Model). All other variables are described in Appendix A. Kolmogorov-Smirnov test: p-value=0.526 for Panel A; p-value=0.911 for Panel B. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

TABLE 4
Regression Results: Audit Quality – Earnings Benchmark

	Panel A: Small Profit				Panel B: Small Increase in Earnings			
Variable	**Coeff.**	**z-statistic**	**p-value**		**Coeff.**	**z-statistic**	**p-value**	
INTERCEPT	1.334	1.54	0.124		1.492	2.52	0.012	**
BREACHED	0.058	0.60	0.545		0.004	0.05	0.958	
POST	0.027	0.21	0.832		0.188	1.12	0.264	
BREACHED x POST	-0.024	-1.75	0.080	*	-0.018	-2.60	0.009	***
BUS_SEG	0.005	0.08	0.935		0.050	0.82	0.410	
GEO_SEG	0.009	1.59	0.113		0.011	1.20	0.230	
LTA	-0.002	-0.54	0.588		-0.006	-1.97	0.049	**
SALESGROWTH	0.039	0.93	0.354		0.021	1.02	0.306	
SALESGROWTH_VOL	0.000	0.59	0.558		0.000	0.17	0.864	
CFO	-0.048	-5.14	0.000	***	-0.066	-0.26	0.794	
CFO_VOL	-0.035	-1.74	0.082	*	-0.049	-1.85	0.065	*
MATWEAK	0.020	1.63	0.091	*	0.085	2.41	0.016	***
LEV	0.043	0.38	0.704		0.054	2.50	0.012	***
LOSS	-1.011	-4.52	0.000	***	-0.823	-4.23	0.000	***
BANKRUPTCY	-0.101	-2.70	0.007	***	-0.035	-3.19	0.001	***
MTB	0.003	1.92	0.055	*	0.000	0.31	0.759	
Industry fixed-effect		Yes				Yes		
Year fixed-effect		Yes				Yes		
Chi-Squared		86.98				106.47		
p-value		0.000				0.000		
Pseudo R-squared		0.29				0.30		
N		2,632				2,632		

This table reports the results of the probit regression analysis for the model presented in Equation (4). Regression coefficients are estimated using the robust cluster technique to correct for heteroscedasticity and serial dependence. *SMALL_PROFIT* (*SMALL_INCREASE*) is the dependent variable in Panel A (Panel B) and it is equal to 1 if a firm reported a net income deflated by lagged total assets (a change in net income deflated by lagged total assets) between 0 and 5 (1.3) percent (Francis and Yu, 2009). All other variables are described in Appendix A. Kolmogorov-Smirnov test: p-value=0.899 for Panel A; p-value=0.992 for Panel B. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

TABLE 5
Regression Results: Audit Quality – Going-Concern Report

Variable	Coeff.	z-statistic	p-value	
INTERCEPT	-3.195	-1.24	0.214	***
BREACHED	-0.521	-1.08	0.282	
POST	-0.374	-0.72	0.471	
BREACHED x POST	0.682	2.87	0.005	***
BUS_SEG	-0.133	-2.42	0.016	**
GEO_SEG	-0.145	-2.05	0.040	**
LTA	-0.067	-4.14	0.000	***
CASH	-0.844	-1.64	0.101	*
PRIOR_GCONCERN	1.760	3.59	0.000	***
REPORT_LAG	0.001	0.23	0.820	
LEV	-0.172	-0.93	0.351	
LOSS	0.302	0.48	0.629	
LAG_LOSS	1.076	2.89	0.004	***
BANKRUPTCY	-0.004	-0.33	0.742	
MTB	0.012	1.25	0.212	
Industry fixed-effect		Yes		
Year fixed-effect		Yes		
Chi-Squared		91.14		
p-value		0.000		
Pseudo R-squared		0.35		
N		2,632		

This table reports the results of the probit regression analysis for the model presented in Equation (5). Regression coefficients are estimated using the robust cluster technique to correct for heteroscedasticity and serial dependence. The dependent variable (*GCONCERN*) is equal to 1 if a firm receives a going-concern audit report and 0 otherwise. All other variables are described in Appendix A. Kolmogorov-Smirnov test: p-value=0.999. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

TABLE 6
Regression Results: Audit Quality – Restatement

Dependent Variable: Restatement

Variable	Coeff.	z-statistic	p-value	
INTERCEPT	-0.798	-1.32	0.188	
BREACHED	0.305	0.34	0.733	
POST	0.315	0.84	0.404	
BREACHED x POST	-0.518	-2.14	0.032	**
LTA	-0.055	-1.64	0.100	*
LEV	0.184	1.25	0.211	
MTB	-0.002	-0.54	0.588	
FIN	-0.027	-0.15	0.883	
EPSGROW	-0.108	-1.25	0.210	
EPR	-0.114	-4.74	0.000	***
CFO	-0.719	-1.13	0.258	
MATWEAK	0.698	2.51	0.012	***
ABAFEES	-0.100	1.05	0.294	
Industry fixed-effect		Yes		
Year fixed-effect		Yes		
Chi-Squared		76.70		
p-value		0.000		
Pseudo R-squared		0.27		
N		2,632		

This table reports the results of the probit regression analysis for the model presented in Equation (6). Regression coefficients are estimated using the robust cluster technique to correct for heteroscedasticity and serial dependence. The dependent variable (*RESTATE*) is equal to 1 if a firm discloses a restatement within the following two years and 0 otherwise (Blankely et al., 2012). All other variables are described in Appendix A. Kolmogorov-Smirnov test: p-value=0.983. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

TABLE 7
Regression Results: SEC Monitoring

	Panel A: SEC Comment Letters			Panel B: SEC Comment Letters (IT)		
Variable	**Coeff.**	**z-statistic**	**p-value**	**Coeff.**	**z-statistic**	**p-value**
INTERCEPT	-2.226	-5.95	0.000 ***	-2.950	-7.64	0.000 ***
BREACHED	0.177	0.28	0.780	-0.424	1.54	0.131
POST	-0.163	-1.55	0.122	-0.991	0.34	0.733
BREACHED x POST	0.417	1.85	0.065 *	0.596	2.84	0.005 ***
MATWEAK	0.239	6.49	0.000 ***	0.277	2.92	0.003 ***
LTA	0.167	8.88	0.000 ***	0.229	4.83	0.000 ***
LOSS	0.041	0.41	0.684	0.057	1.27	0.204
HIGHBANKRUPTCY	0.138	0.61	0.542	0.253	0.87	0.387
SALEGROWTH	0.334	2.67	0.008 ***	0.163	2.21	0.027 **
BUS_SEG	0.253	0.50	0.618	0.262	2.11	0.035 **
Industry fixed-effect		Yes			Yes	
Year fixed-effect		Yes			Yes	
Chi-Squared		84.01			82.73	
p-value		0.000			0.000	
Pseudo R-squared		0.38			0.35	
N		2,632			2,632	

This table reports the results of the probit regression analysis for the model presented in Equation (7). Regression coefficients are estimated using the robust cluster technique to correct for heteroscedasticity and serial dependence. The dependent variable in Panel A (Panel B) is equal to 1 if a firm receives an SEC Comment Letter (IT-related SEC Comment Letter) within the following two years, 0 otherwise. All other variables are described in Appendix A. Kolmogorov-Smirnov test: p-value= 0.632 for Panel A; p-value= 0.973 for Panel B. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

APPENDIX A
Variable Definitions

Variable	Description	Data Source
Dependent Variables		
TA	Total accruals estimated as the change in non-cash current assets minus the change in current liabilities (excl. the current portion of long-term debt), minus depreciation and amortization, scaled by lagged total assets (Kothari et al., 2005).	Compustat
ABS_ACC_JM	Absolute value of abnormal accruals estimated using the Modified Jones Model (Kothari et al., 2003).	Compustat
ABS_ACC_DD	Absolute value of abnormal accruals estimated using the Dechow-Dichev Model (Dechow and Dichev, 2002).	Compustat
SMALL_PROFIT	Indicator variable equal to 1 if a firm reported a net income, deflated by lagged total assets, between 0 and 5 percent (Francis and Yu, 2009).	Compustat
SMALL_INCREASE	Indicator variable equal to 1 if a change in net income, deflated by lagged total assets, lies between 0 and 1.3 percent (Francis and Yu, 2009).	Compustat
GCONCERN	Indicator variable equal to 1 if a firm receives a going-concern audit report, 0 otherwise (Francis and Yu, 2009).	Audit Analytics
RESTATE	Indicator variable equal to 1 if a firm announces a restatement within the following two years, 0 otherwise (Blankely et al., 2012).	Audit Analytics
CL	Indicator variable equal to 1 if a firm receives an SEC Comment Letter within the following two years, 0 otherwise.	Audit Analytics
CL_IT	Indicator variable equal to 1 if a firm receives an SEC Comment Letter on "Data Protection and Security Breach" within the following two years, 0 otherwise.	Audit Analytics
BREACH	Indicator variable equal to 1 if a firm experiences a cyber-security incident in year t, and 0 otherwise.	Privacy Rights Clearinghouse
Explanatory Variables		
BREACHED	Indicator variable equal to 1 if a firm belongs to the treatment sample i.e. it experienced a cyber-security incident, 0 otherwise.	Privacy Rights Clearinghouse
POST	Indicator variable equal to 1 if firm-year belongs to the post-incident period, 0 otherwise.	
BREACHEDxPOST	Interaction variable between *BREACHED* and *POST*. Difference-in-difference estimator.	
ΔREV	Change in revenues between year t-1 and year t (Kothari et al., 2005).	Compustat
PPE	Gross property, plant, and equipment (Kothari et al., 2005).	Compustat
NI	Operating income after depreciation (Khotari et al., 2005)	Compustat
LAF	Natural logarithm of audit fees.	Audit Analytics
ABAFEES	Abnormal audit fees estimated as per Blankley et al. (2012).	
PRIOR_GCONCERN	Indicator variable equal to 1 if a firm received a going-concern opinion in the previous fiscal year, 0 otherwise.	Audit Analytics

APPENDIX A (continued from previous page)
Variable Definitions

Variable	Description	Data Source
LEV	Total debt divided by total assets.	Compustat
LOSS	Indicator variable equal to 1 if the income before extraordinary items is lower than zero, 0 otherwise.	Compustat
LAG_LOSS	Indicator variable equal to 1 if a firm reported a loss in the previous fiscal year, 0 otherwise.	Compustat
BANKRUPTCY	Altman (2000) Z-Score.	Compustat
HIGHBANKRUPTCY	Indicator variable equal to 1 if a firm is assigned to the decile having the lowest Altman's Z-Score, 0 otherwise.	Compustat
SALESGROWTH	One-year growth rate of a firm's sales revenue.	Compustat
SALESGROWTH_VOL	Standard deviation of sales revenue for the most recent three fiscal years.	Compustat
BUS_SEG	Number of business segments a firm operates in as reported in the Compustat segments database.	Compustat
GEO_SEG	Number of geographical segments a firm operates in as reported in the Compustat segments database.	Compustat
MTB	Market-to-book ratio.	Compustat
FIN	Sum of additional cash raised from issuance of long-term debt, common stock and preferred stock divided by total assets.	Compustat
EPSGROW	Indicator variable equal to 1 if a firm experiences a positive earnings change for four consecutive quarters, 0 otherwise.	Compustat
EPR	Earnings-to-price ratio, defined as income from continuing operations scaled by market capitalisation at the end of the fiscal year.	Compustat
CFO	Cash flow from operations.	Compustat
CFO_VOL	Standard deviation of cash flows from operations for the most recent three fiscal years.	Compustat
MATWEAK	Indicator variable equal to 1 if a firm receives a material weakness opinion in the current or in the following year, 0 otherwise.	Audit Analytics
REPORT_LAG	Number of days between the fiscal year-end and the earnings announcement date.	Compustat
CASH	Sum of the firm's cash and investment securities, scaled by total assets.	Compustat
LTA	Natural logarithm of end of year total assets.	Compustat
SIZE	Natural logarithm of end of year market capitalisation.	Compustat
AGE	Natural logarithm of 1 plus the number of years the firm is listed on Compustat.	Compustat
ROA	Return on assets calculated as net income at fiscal year end scaled by total assets.	Compustat
SEGMENTS	Natural logarithm of 1 plus the number of operating and geographic segments.	Compustat
ACQUISITIONS	The aggregate dollar value of acquisitions in the fiscal year *t-1*, scaled by market capitalisation at the end of year *t*.	Compustat

APPENDIX A (continued from previous page)
Variable Definitions

Variable	Description	Data Source
SPECIALIST	Indicator variable equal to 1 if the firm's auditor has the highest audit fees' market share in the client's industry, 0 otherwise.	Audit Analytics
Industry Indicators	Industry indicators based on 2-digit SIC Codes.	Compustat
Year Indicators	Fiscal years indicators	Compustat

APPENDIX B

Regression Results: Audit Fee Model

Variable	Coeff.	t-statistic	p-value	
INTERCEPT	6.450	182.34	0.000	***
LTA	0.486	237.15	0.000	***
CR	0.000	-1.74	0.080	*
CA_TA	0.453	20.67	0.000	***
ARINV	-0.039	-1.65	0.100	
ROA	-0.002	-5.00	0.000	***
LOSS	0.153	19.86	0.000	***
FOREIGN	0.390	51.81	0.000	***
MERGER	0.077	8.85	0.000	***
BUSY	-0.081	-10.87	0.000	***
LEV	0.001	1.76	0.079	*
INTANG	0.306	14.34	0.000	***
SEG	0.136	28.79	0.000	***
MATWEAK	0.373	18.90	0.000	***
Industry fixed-effect		Yes		
Year fixed-effect		Yes		
F-statistic		131.32		
p-value		0.000		
R-squared		0.77		
N		44,193		

This table reports the results of the regression analysis for the model proposed by Blankley et al. (2012) to estimate abnormal audit fees. Regression coefficients are estimated using the robust cluster technique to correct for heteroscedasticity and serial dependence. The dependent variable is the natural logarithm of audit fees (*LAF*). All other variables are described in Appendix A. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

APPENDIX C (I)
Pearson Correlation Coefficients between Variables

Variable	CL		CL_IT		ABS_ACC_JM		ABS_ACC_DD		SMALL_PROFIT		SMALL_INCREASE		GCONCERN	
CL	1.000													
CL_IT	0.060	***	1.000											
ABS_ACC_JM	-0.023		0.085	***	1.000									
ABS_ACC_DD	-0.087	***	0.070	***	0.908	***	1.000							
SMALL_PROFIT	-0.072	***	-0.002		0.033	*	-0.009		1.000					
SMALL_INCREASE	-0.073	***	0.004		-0.039	**	-0.043	**	0.155	***	1.000			
GCONCERN	0.015		-0.008		-0.010		-0.010		0.061	***	-0.040	***	1.000	
PRIOR_GCONCERN	0.000		-0.008		-0.008		-0.009		0.050	***	-0.039	**	0.613	***
RESTATE	0.019		0.033	**	0.022		0.032	**	-0.004		-0.051	***	-0.024	*
LAF	0.051	***	0.069	***	-0.076	***	-0.116	***	0.154	***	0.122	***	-0.014	
ABAFEES	0.021		0.009		-0.024		-0.020		0.077	***	0.040	**	-0.004	
LTA	0.074	***	0.067	***	-0.043	**	-0.087	***	0.237	***	0.218	***	-0.010	
LEV	-0.049	***	-0.014		0.029	*	0.077	***	0.076	***	-0.074	***	0.034	**
LOSS	0.012		-0.035	**	-0.005		-0.031	*	0.328	***	-0.188	***	0.107	***
LAG_LOSS	-0.009		-0.014		-0.015		-0.046	**	0.256	***	-0.134	***	0.092	***
BANKRUPTCY	-0.009		-0.005		-0.008		0.018		-0.297	***	-0.022		-0.096	***
HIGHBANKRUPTCY	0.003		-0.005		-0.001		0.003		-0.146	***	-0.068	***	-0.011	
SALESGROWTH	0.085	***	0.001		0.047	**	0.039	**	-0.061	***	0.011		-0.056	***
SALESGROWTH_VOL	0.074	***	0.060	***	-0.027		-0.019		-0.039	**	0.029	**	-0.013	
BUS_SEG	-0.027	*	0.018		-0.035	**	-0.060	**	-0.039	**	-0.016		-0.043	***
GEO_SEG	-0.016		0.012		-0.103	***	-0.106	***	-0.163	***	-0.112	***	-0.024	*
MTB	-0.021		0.015		0.001		0.007		-0.044		0.007		-0.010	
FIN	0.011		-0.027	*	0.008		0.036		-0.012	***	-0.079	***	0.016	
EPSGROW	-0.078	***	0.031	**	-0.003		0.003	*	-0.091	***	0.461	***	-0.033	**
EPR	-0.014		-0.006		-0.017		-0.023		0.057	***	0.071	***	-0.007	
CFO	0.011		0.007		-0.038	**	-0.024		-0.225	***	-0.034	**	-0.056	***
CFO_VOL	0.003		-0.009		0.048	**	0.051	***	-0.015		-0.058	***	0.025	*
MATWEAK	0.014		-0.009		0.038	**	0.014		0.048	***	-0.050	***	-0.013	
REPORT_LAG	0.052	***	0.009		0.005		-0.007		-0.035	**	-0.054	***	0.001	
CASH	0.028	*	-0.001		0.051	**	0.041	**	-0.070	***	-0.053	***	-0.001	

This table reports the Pearson correlation coefficients among variables adopted in the empirical analysis.
All the variables are defined in Appendix A. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

APPENDIX C (II)
Pearson Correlation Coefficients between Variables

Variable	PRIOR_GCONCERN		RESTATE		LAF		ABAFEES		LTA		LEV		LOSS	
CL														
CL_IT														
ABS_ACC_JM														
ABS_ACC_DD														
SMALL_PROFIT														
SMALL_INCREASE														
GCONCERN														
PRIOR_GCONCERN	1.000													
RESTATE	-0.024		1.000											
LAF	-0.033	**	-0.055	***	1.000									
ABAFEES	-0.036	**	-0.028	*	0.633	***	1.000							
LTA	-0.016		-0.091	***	0.807	***	0.165	***	1.000					
LEV	0.050	***	0.029	**	-0.033	**	0.055	***	-0.089	***	1.000			
LOSS	0.121	***	0.032	**	-0.070	***	-0.045	***	-0.140	***	0.126	***	1.000	
LAG_LOSS	0.108	***	0.024		-0.092	***	-0.024		-0.150	***	0.127	***	0.497	***
BANKRUPTCY	-0.168	***	-0.044	**	-0.067	***	-0.122	***	0.005		-0.287	***	-0.248	***
HIGHBANKRUPTCY	-0.011		-0.016		-0.123	***	-0.083	***	-0.138	***	-0.113	***	-0.048	***
SALESGROWTH	-0.011		-0.010		-0.089	***	-0.113	***	-0.076	***	0.013		-0.034	**
SALESGROWTH_VOL	-0.013		-0.070	***	0.438	***	0.004		0.283	***	-0.081	***	-0.067	***
BUS_SEG	-0.050	***	-0.004		0.231	***	0.062	***	0.065	***	0.032	**	-0.027	**
GEO_SEG	-0.030	**	0.026	*	0.251	***	0.097	***	-0.051	***	0.014		0.014	
MTB	-0.006		-0.011		0.005		0.007		-0.005		-0.001		-0.022	
FIN	0.019		0.038	**	-0.135	**	-0.014		-0.191	***	0.382	***	0.079	***
EPSGROW	-0.046	***	-0.072	***	0.040		0.069	***	0.009		-0.026	*	-0.204	***
EPR	-0.008		0.002		0.002	***	-0.004		0.046	***	0.029	*	-0.040	**
CFO	-0.060	***	-0.025		-0.041	***	-0.011		-0.066	***	-0.029	**	-0.133	***
CFO_VOL	0.027	*	0.034	**	-0.154		-0.119	***	-0.136	***	-0.011		0.056	***
MATWEAK	-0.013		0.150	***	0.014		-0.055	***	-0.021		0.055	***	0.085	***
REPORT_LAG	0.014		-0.005		-0.116	***	-0.107	***	-0.104	***	-0.005		0.092	***
CASH	-0.002		0.008		-0.085	***	-0.115	***	-0.106	***	-0.056	***	0.025	*

This table reports the Pearson correlation coefficients among variables adopted in the empirical analysis.
All the variables are defined in Appendix A. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

APPENDIX C (III)
Pearson Correlation Coefficients between Variables

Variable	LAG_LOSS		BANKRUPTCY		HIGHBANKRUPTCY		SALESGROWTH		SALESGROWTH_VOL		BUS_SEG		GEO_SEG	
CL														
CL_IT														
ABS_ACC_JM														
ABS_ACC_DD														
SMALL_PROFIT														
SMALL_INCREASE														
GCONCERN														
PRIOR_GCONCERN														
RESTATE														
LAF														
ABAFEES														
LTA														
LEV														
LOSS														
LAG_LOSS	1.000													
BANKRUPTCY	-0.243	***	1.000											
HIGHBANKRUPTCY	-0.048	***	0.558	***	1.000									
SALESGROWTH	0.036	**	-0.082	***	0.059	***	1.000							
SALESGROWTH_VOL	-0.069	***	0.036	**	-0.050	***	0.008		1.000					
BUS_SEG	-0.028	*	-0.065	***	-0.056	***	-0.042	***	0.093	***	1.000			
GEO_SEG	0.007		0.076	***	0.072	***	-0.027	**	0.082	***	0.164	***	1.000	
MTB	-0.019		0.034	*	0.020		0.008		-0.001		0.016		0.001	
FIN	0.045	***	-0.069	***	-0.012		0.054	***	-0.085	***	-0.026	*	0.017	
EPSGROW	0.098	***	0.049	**	0.022		0.104	***	0.014		0.021		0.009	
EPR	-0.042	**	-0.034	*	-0.018		0.009		0.007		-0.034	**	-0.088	***
CFO	-0.112	***	0.285	***	0.057	***	-0.016		-0.006		0.003		0.077	***
CFO_VOL	0.060	***	-0.154	***	0.019		0.164	***	-0.034	**	-0.037	**	-0.040	***
MATWEAK	0.064	***	-0.035	**	-0.020		0.016		0.018		0.019		0.023	
REPORT_LAG	0.077	***	-0.019		0.000		0.031	**	0.005	***	-0.047	***	-0.024	*
CASH	0.029	**	0.252	***	0.097	***	0.252	***	-0.020	**	-0.028	*	0.025	*

This table reports the Pearson correlation coefficients among variables adopted in the empirical analysis.
All the variables are defined in Appendix A. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

APPENDIX C (IV)
Pearson Correlation Coefficients between Variables

Variable	MTB	FIN	EPSGROW	EPR	CFO	CFO_VOL	MATWEAK
CL							
CL_IT							
ABS_ACC_JM							
ABS_ACC_DD							
SMALL_PROFIT							
SMALL_INCREASE							
GCONCERN							
PRIOR_GCONCERN							
RESTATE							
LAF							
ABAFEES							
LTA							
LEV							
LOSS							
LAG_LOSS							
BANKRUPTCY							
HIGHBANKRUPTCY							
SALESGROWTH							
SALESGROWTH_VOL							
BUS_SEG							
GEO_SEG							
MTB	1.000						
FIN	0.000	1.000					
EPSGROW	0.022	-0.039 **	1.000				
EPR	-0.005	-0.007	-0.053 ***	1.000			
CFO	0.018	-0.016	0.053 ***	-0.017	1.000		
CFO_VOL	0.002	0.045 ***	-0.020	-0.009	0.289 ***	1.000	
MATWEAK	-0.008	0.049 ***	-0.023 *	0.023	-0.017	-0.002 ***	1.000
REPORT_LAG	-0.009	0.045 ***	-0.055 ***	-0.016	-0.015	0.039	0.059 ***
CASH	0.011	0.036 **	-0.004	-0.021	0.791 ***	0.376 ***	-0.002

This table reports the Pearson correlation coefficients among variables adopted in the empirical analysis.
All the variables are defined in Appendix A. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.

APPENDIX C (V)
Pearson Correlation Coefficients between Variables

Variable	REPORT_LAG		CASH
CL			
CL_IT			
ABS_ACC_JM			
ABS_ACC_DD			
SMALL_PROFIT			
SMALL_INCREASE			
GCONCERN			
PRIOR_GCONCERN			
RESTATE			
LAF			
ABAFEES			
LTA			
LEV			
LOSS			
LAG_LOSS			
BANKRUPTCY			
HIGHBANKRUPTCY			
SALESGROWTH			
SALESGROWTH_VOL			
BUS_SEG			
GEO_SEG			
MTB			
FIN			
EPSGROW			
EPR			
CFO			
CFO_VOL			
MATWEAK			
REPORT_LAG	1.000		
CASH	0.028	*	1.000

This table reports the Pearson correlation coefficients among variables adopted in the empirical analysis.
All the variables are defined in Appendix A. *, **, *** denote significance at 10, 5 and 1 percent levels, respectively.